PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

DECLARACIÓN Y AUTORIZACIÓN

Yo, LUIS HUMBERTO VÁSQUEZ VILLACRESES, con cedula de ciudadanía C.C.: 1712132651, autor del trabajo de graduación intitulado: "Herramientas de seguridad de la información en dispositivos finales y móviles con relación a "BYOD" – Caso de estudio de la plataforma IBM Security Endpoint Manager", previa a la obtención del título profesional de INGENIERO EN SISTEMAS Y COMPUTACIÓN, en la Facultad de INGENIERÍA.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistemas Nacional de Información de la Educación Superior del Ecuador para su difusión publicación respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE, el referido trabajo de graduación, respetando las políticas de propiedad intelectual.

Quito, abril 2015

Luis Humberto Vásquez Villacreses

C.C.: 1712132651

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS Y COMPUTACIÓN

"HERRAMIENTAS DE SEGURIDAD DE LA INFORMACIÓN EN DISPOSITIVOS FINALES Y MÓVILES CON RELACIÓN A "BYOD" – CASO DE ESTUDIO DE LA PLATAFORMA IBM SECURITY ENDPOINT MANAGER."

AUTOR
LUIS HUMBERTO VÁSQUEZ VILLACRESES

DIRECTOR
Ph.D. GUSTAVO CHAFLA ALTAMIRANO

QUITO, 2015

DEDICATORIA

Esta disertación está dedicada a mis padres por estar conmigo, por enseñarme a crecer y a que si caigo debo levantarme, por apoyarme y guiarme, por ser las bases que me ayudaron a llegar hasta aquí.

De igual forma, la dedico a mi familia, a mi esposa y suegros, quienes me han dado fortaleza. Sin ayuda de ellos no hubiera logrado ningún objetivo, tanto académico como personal.

El presente trabajo está dedicado a mi hermano Roberth Iván, cuyo esfuerzo me motiva a seguir este trabajo, el cual no inicia ni termina con la presente disertación.

AGRADECIMIENTOS

Agradezco de manera particular a mis padres, y a mi esposa por todo el apoyo brindado durante la carrera y en la elaboración del presente trabajo.

Así mismo agradezco, al Ingeniero Gustavo Chafla Altamirano, quién fue el tutor de la presente disertación; por ser un profesional muy dedicado y quien con su conocimiento teórico y práctico del tema, me incentivó a conocer más.

Finalmente, agradezco a la Pontificia Universidad Católica del Ecuador y a todo su personal docente y administrativo, porque durante toda la carrera me incentivaron al estudio y conocimiento de esta rama tan importante.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

RESUMEN

La disertación pretende analizar las vulnerabilidades en los sistemas de información frente al nuevo fenómeno global que se está produciendo en nuestra sociedad, una tendencia que en el día a día tienen que tratar miles de empresas y que coloca en varios apuros a las distintas autoridades de TI.

El fenómeno de BYOD conocido como “Bring Your Own Device” se trata de millones de usuarios la gran mayoría empleados que adquieren avanzados dispositivos móviles como son smartphones y tablets para su uso personal que conjuntamente las adecuan con aplicaciones que ayudan a gestionar de mejor manera su acciones laborales ya sea mediante el uso del correo de la empresa o como la gestión de archivos e información crítica de la misma.

El análisis de algunas herramientas que permiten administrar estos dispositivos nos ayuda a conocer la prevalencia de esta tendencia en las empresas, de igual manera se puede observar como las empresas hacen frente a esta tendencia y que tipos de seguridades son las más adecuadas a los diferentes ambientes de trabajo ya sea en estaciones de trabajo como dispositivos móviles. Frente a la realidad del tratamiento de la información de un lugar de trabajo cada vez más móvil, las organizaciones luchan por encontrar el equilibrio entre el empoderamiento de los empleados con los dispositivos móviles para que puedan ser más productivos y la protección de su información confidencial y personal sin incurrir en grandes gastos mientras se implementan soluciones integrales y completas.

En el mercado de seguridad de la información existen muchas plataformas que permiten cubrir las necesidades de las empresas de las cuales se seleccionará al fabricante IBM con su solución de Endpoint Manager debido a que es una solución robusta que es entregada por una empresa líder en el mercado.

Finalmente para la implementación y despliegue de la plataforma se creará una guía de dimensionamiento e instalación en la cual se podrá observar los requerimientos mínimos de los sistemas así como los beneficios que se obtienen al configurar adecuadamente una plataforma de seguridad frente a la inversión que debe afrontar inicialmente las empresas para complementar y fortalecer las políticas de seguridad respecto a la tendencia BYOD.

INTRODUCCIÓN

Hoy en día se habla de empresas interconectadas, de ciudades automatizadas; en general de un mundo inteligente del cual todos somos usuarios y esto conlleva a nuevos problemas de seguridad para todas las empresas donde cada usuario intercambia información crítica desde sus dispositivos personales.

Las tendencias del uso de dispositivos móviles ha marcado un cambio en la manera de operar de las empresa volviéndolas más sociales, logrando crear una disciplina de colaboración con clientes y entre empleados dando a los usuarios más libertad para elegir sus herramientas de trabajo, sin un control responsable logrando exponer cada organización a las amenazas que se encuentran en nuestro medio informático, por tal motivo se hace necesario aplicar soluciones globales y completas que cubran todo el portafolio de dispositivos que se manejan en las empresas.

La demanda creciente de acceso a las redes de información en cualquier lugar y en cualquier momento ha creado innovaciones en la forma de trabajar pero a la vez descubre riesgos para los departamentos de seguridad de información de las empresas. Por tal motivo, es importante aprovechar las ventajas del crecimiento y sociabilización de la información pero a su vez es necesario tomar las medidas preventivas necesarias para garantizar la protección de la información crítica de las empresas y personal de sus empleados.

El tema de la presente disertación surgió como resultado de mi experiencia y capacitación profesional que he tenido por parte de IBM y Symantec para la implementación de soluciones de seguridad de la información, en donde tuve la oportunidad de profundizar mis conocimientos en varias áreas de trabajo como son la prevención de perdida de información, la distribución de identidades o federación de usuarios y manejo de riesgo y gobernabilidad de la información.

La incorporación de dispositivos tecnológicos de los trabajadores en el ámbito profesional va más allá de un ámbito de seguridad y prevención; es un conjunto de normas que permite educar al usuario que en conjunto con las herramientas adecuadas se puede integrar a las empresas para potencia la eficiencia de los empleados.

Durante la elaboración de este tema se abordaran los riesgos que implica la adopción de este nueva tendencia en las empresas, como afecta el ingreso de dispositivos personales a la red de seguridad y gobernabilidad de TI; de igual manera se afianzará los conocimientos

de la arquitectura de las herramientas de seguridad basadas en el entorno cliente – servidor, la misma que se pudo estudiar en la carrera de Ingeniería de Sistemas. Se toma en cuenta cuáles son sus funcionalidades y que beneficios presenta en el despliegue en el área de trabajo. Adicionalmente se puede ver las características principales de algunas herramientas de seguridad existentes en el mercado.

Varias plataformas han ido surgiendo para solventar la seguridad en los dispositivos finales, entendiéndose que un dispositivo final o "endpoint" son todos aquellos equipos individuales que se extienden más allá del perímetro de una red, estos pueden ser los computadores de escritorio, portátiles, teléfonos inteligentes y tablets. Las plataformas más conocidas para asegurar estos dispositivos están distribuidas acorde a las características y rango de protección que pueden brindar, logrando así ajustarse a los ambientes cambiantes de las empresas de hoy en día. En este tipo de plataformas se puede observar la aparición de un nuevo modelo de gestión de seguridad basado en la nube de internet, en el cual ya no se ocupan los recursos físicos de la empresa sino que se adquiere la solución o herramienta como un servicio estandarizado de forma flexible y adaptativa.

Se podrá observar un análisis de las características más notables de seis productos que se apegan a dos modelos de licenciamiento siendo tres herramientas para el modelo de prestación de servicios, conocido como SaaS (Software como servicio) y tres herramientas cuyo modelo de adquisición es de forma local o en sitio.

Tras un análisis de algunos de los fabricantes más renombrados en la creación de soluciones de seguridad se hará énfasis en la herramienta de IBM debido a las características que presenta su plataforma y la amplia gama de productos que soporta su solución desde dispositivos móviles hasta puntos y quioscos de venta dando una visibilidad y control de la información de extremo a extremo.

Para finalizar esta disertación se realizara una guía de instalación y dimensionamiento de la herramienta que permitirá realizar la implementación de la misma en la cual se podrá observar los requerimientos mínimos de los sistemas así como los beneficios que se obtienen al integrar cada uno de sus módulos, logrando presentar una solución granular, escalable y robusta que fortalece las políticas de seguridad respecto a la tendencia BYOD en las empresas.

CAPÍTULO 1. MARCO TEÓRICO

1.1. INTRODUCCIÓN A BYOD.

BYOD es la tendencia tecnológica, el modelo global que enmarca la movilidad empresarial lo cual implica que los usuarios o trabajadores utilicen sus propios dispositivos ya sean estos smartphones, tablets y laptops para realizar tareas corporativas y personales presentando como ventajas la flexibilidad y efectividad en el trabajo otorgando una mayor productividad a largo plazo, optimizando la relación que existe entre el tiempo que las personas la dedican a sus tareas en las empresas y su vida personal.

Durante este capítulo se va a tratar los conceptos básicos para entender de mejor manera las estrategias y reglamentos que existen para tomar una postura de seguridad proactiva y no reactiva al igual que la arquitectura inicial con la que trabajan la mayoría de los fabricantes de soluciones de seguridad de la información en el mercado.

1.1.1. Tendencia BYOD.

Los dispositivos actualmente cuentan con diferentes interfaces que son intuitivas y de fácil uso, permitiendo el acceso a una gran cantidad de aplicaciones, las mismas que no son solo para uso personal o entretenimiento sino para negocio con lo cual más personas son las que integran sus dispositivos al flujo de trabajo diario innovando su forma de trabajar y permitiendo a las empresas así un ahorro en infraestructura. Las empresas se evitan la adquisición de nuevos dispositivos, la implementación de software propio, licenciamiento y mantenimiento de estos equipos. Por otro lado el usuario promedio actualiza sus dispositivos móviles personales con mayor regularidad que las empresas, otorgando el beneficio de las últimas características y capacidades a las empresas.

Debido al gran crecimiento que se ha dado en los últimos años los dispositivos móviles han experimentado grandes cambios logrando que los usuarios aprovechen las características de portabilidad y las facilidades de interconectividad para utilizarlos como herramientas de trabajo e integrándolas con las redes sociales creando una nueva forma de trabajar, planteado nuevas oportunidades y riesgos para las empresas. Esta interconectividad en las empresas ha dado lugar a la evolución de las herramientas creando nuevas plataformas de colaboración donde cada usuario interactúa con los demás para mejorar su trabajo habitual y sociabilizarlos con el resto mediante el uso de servicios en la nube.

Durante los últimos años varias herramientas han ido surgiendo para tratar de dar solución a la manera de cómo salvaguardar los datos confidenciales de las empresas, algunas centradas a la perdida de información, otras diseñadas para la ubicación de los dispositivos perdidos, algunas con más beneficios que otras; con lo cual, en conjunto se ha tratado de tener un control de la información que manejan las empresas y que es crítico en el giro del negocio. A pesar que la protección y confidencialidad de los datos es uno de los desafíos más importantes de BYOD, se debe tener en cuenta un enfoque más amplio el cual involucre a los usuarios, sus dispositivos, la administración de los mismos y la gestión de las aplicaciones que estos contienen. Este análisis debe estar dado por los requisitos, capacidades y diseño de la infraestructura

1.1.2. Estrategias y consideraciones de BYOD.

Las empresas de hoy en día tienen que hacer frente a la tendencia "Bring Your Own Device", que a pesar de que no es una práctica reciente, ha ido incrementando su aplicación y uso de manera rápida debido a la evolución de la tecnología y al crecimiento del mercado de los dispositivos móviles ya sean smartphones y tablets. Pero con esta tendencia ha llegado un nuevo desafío para los gerentes de sistemas lo cual es tener la capacidad de administrar un grupo de dispositivos que no mantienen estándares, con diferentes versiones de sistemas operativos, con una variedad de niveles de seguridad, con múltiples aplicaciones que se integran con las cuentas de los usuarios y que pueden tener acceso a todos los recursos empresariales al ser conectados en las redes internas de las empresas. "Frente a esta situación los gerentes de sistemas afirman que tienen tres opciones, o estrategias que pueden tomar para afrontar esta tendencia:

- No permitir BYOD.
- Establecer estrictas políticas empresariales para los accesos de los equipos a la red corporativa.
- Adquirir una solución de administración de seguridad y soporte por parte de una compañía de confianza." (Software Guru, 2013)

Sin embargo, la implementación de estas estrategias implica la adaptación de las aplicaciones y de la infraestructura que la empresa tenga en ese momento; comunicaciones unificadas, almacenamiento, sistema de respaldos entre otros. Inicialmente se debe comprender que esta tendencia implica riesgos si no se la aplica de manera adecuada, pero

de igual manera representa una ventaja para aumentar la productividad dentro del giro del negocio si se lo ve como una ventaja competitiva donde las empresas podrán exponer sus aplicaciones a un ambiente móvil con un control adecuado de ser necesario mediante la implementación de un MDM[1] o Endpoint Manager[2] dando a la empresa una mayor seguridad de operación.

Las consideraciones que se deberán tomar para una correcta administración de dispositivos finales y móviles inicia con la implementación de políticas de seguridad y de acceso a la red corporativa claras, las mismas que deben ser redactadas en un documento que se pueda sociabilizar con todos los empleados de tal forma que el personal conozca lo que puede hacer al ocupar sus dispositivos. Al tener un proceso de control de accesos a los sistemas críticos de la empresa la gerencia de TI asegura conocer el perfil del empleado que está solicitando los accesos y así asignarle diferentes niveles y perfiles de acceso para salvaguardar dicha información.

Este fenómeno está en incremento constante motivado no solo por el desarrollo tecnológico sino también por las oportunidades que brinda tanto a las empresas como a los empleados. Las compañías de hoy en día deben considerar el ahorro de costos que incurre puesto que las organizaciones no tienen que adquirir estos dispositivos o financiarlos mediante leasing[3], cubrir seguros de robo, asumir el deterioro de los equipos o la obsolescencia tecnológica. Al permitir la incorporación de estos dispositivos se obtiene una mejora de la productividad y mejores condiciones de trabajo, lo cual está ligado a una mayor satisfacción de los empleados los cuales pueden considerar un privilegio el poder utilizar sus propios dispositivos y aplicaciones. Según algunos estudios realizados por DELL (DELL, 2013), revelan que el 74% de las organizaciones han experimentado una mejora en la productividad de los empleados, mientras que el 70% ha mejorado los tiempos de respuesta a los clientes.

Se puede considerar que las empresas tienen muchas ventajas si desarrollan las actividades de BYOD en donde predomina la diversidad generada por el empleado; todo

[1] (Darnalt C. , 2013) **MDM:** Es una herramienta de software que permite monitorear, gestionar dispositivos móviles sin tomar en cuenta el proveedor de servicios.
[2] (Darnalt C. , 2013) **Endpoint Manager:** Es una herramienta de software que permite la administración y gestión de los activos de TI.
[3] (IBM Global Financing, 2015) **Leasing:** Se lo conoce como un arrendamiento de equipos informáticos con derecho de compra, bajo este concepto al finalizar el plazo determinado el adquiriente puede comprar dichos equipos.

esto apoyado con la herramienta consultiva que apoya, define y mejora los procesos de seguridad vigentes. BYOD no tiene que ser una conducta, sino una ventaja competitiva que requiere un control adecuado por parte de la gerencia de TI.

1.1.3. Reglamentos de propiedad intelectual.

Para lograr implementar un entorno BYOD regulado, controlado y que sea eficaz; resultando en un ahorro para la empresa pero a su vez logrando la convivencia y la interconectividad del empleado con sus dispositivos personales con fines incrementar su productividad se debe tener en cuenta las implicaciones legales que este tema conlleva. Como es el caso de disponer del consentimiento del usuario para el usos de su dispositivo con aplicaciones corporativas y refrendarlo mediante un escrito. De igual manera se debe tomar en cuenta los reglamentos de derechos de autor que se aplican en la seguridad de la información y que está protegida por las leyes nacionales y las normativas internacionales que operan en el Sur Global[4]. Estos reglamentos de propiedad intelectual tienen como objetivo familiarizar a las personas con el modo general que opera el derecho de autor. (Story, 2009).

El derecho de autor es un sistema legal que regula la creación, propiedad, control y uso por el público de productos resultantes de ciertas actividades creativas o no tan creativas regidas por la inteligencia humana (Story, 2009); estas actividades toman el nombre de obras las mismas que pueden ser tituladas y protegidas contra la copia o modificación y que solo el autor con su consentimiento o disposición legal lo permita disponible llamándolo “derecho de usuario”.

La presencia y proceso de las nuevas tecnologías de la información (TIC’s) en la Sociedad de la Información y Comunicación (SIC), ha dado lugar al surgimiento de nuevas actividades y figuras jurídicas legales e ilegales. Entre estas se encuentra el delito informático, el cual consiste en la vulneración de los derechos de autor mediante la apropiación de algo ajeno con fines de lucro; la vulneración se la puede realizar mediante una distribución de correo con avisos publicitarios o correo malicioso todos realizados a través de hardware y software destinados para invadir, dañar o destruir un sistema de propiedad ajena, sea empresa, gobierno o personal, pudiendo abarcar asuntos relacionados

[4] (Story, 2009) **Sur Global:** Son los “países en desarrollo” contemplados por los países de Latinoamérica, África y Asia.

con la información, comunicación personal, actividades económicas y funcionamiento con internet. (Zambrano, 2012). Se debe aclarar que un delito informático atenta los bienes intangibles y privados que puede ser desde el registro del nombre de dominio de una empresa o persona natural hasta el hurto de conocimiento de cualquier índole mediante el fraude o sabotaje informático.

Según la gravedad de los delitos y en relación al contenido o finalidad y a la infracción a los derechos de propiedad intelectual que realizan se los puede clasificar en:

- *Phishing:* consiste en él envió de correos electrónicos que simulan ser originales o pertenecer a fuentes confiables ya sean entidades bancarias y cuya finalidad es apropiarse de los datos privados de los usuarios como pueden ser las credenciales de acceso o números de cuentas y tarjetas.
- *Tampering:* es la modificación sin autorización de datos o código de software para la manipulación del sistema objetivo (victima), con la finalidad de alterar, obtener o borrar información causando la falla general del sistema y en el peor de los casos inhabilitándolo.
- *Scanning:* es uno de los métodos que lleva mucho tiempo en uso y se encarga de explorar y descubrir puntos de comunicación susceptibles y que son de utilidad para el objetivo en particular. La metodología varía acorde las técnicas, puertos y protocolos soportados.
- *Pharming:* consiste en enviar al usuario a una página falsa para apropiarse de las credenciales o información crítica o personal, es similar al phishing pero tiene una metodología más avanzada en la que ya no se engaña al usuario mediante correo o links de visita sino que engaña al equipo objetivo para que resuelva las URL correctas hacia direcciones maliciosas o fraudulentas.
- *Skimming:* es la técnica mediante la cual se trata de obtener las credenciales de las tarjetas de crédito del usuario ya sea mediante el uso de software o hardware durante la transacción facilitando la clonación de tarjetas o el ingreso a la información bancaria para realizar transacciones fraudulentas. (Goncalves, 1997, pág. 25)

Los sujetos que realizan los delitos informáticos, son personas que tienen conocimientos avanzados de la informática que buscan lucrar mediante el uso de varias técnicas con finalidad de la sustracción de la información. Es necesario que los empleados de las empresas conozcan los medios por los cuales pueden ser víctimas y salvaguardar la

información tanto personal como laboral que poseen. Acorde a las leyes de propiedad intelectual y propiedad de autor mediante conceptos generales y universales originados desde las mismas Naciones Unidades, cuya comisión especializada, UNCITRAL o CNUDMI, elaboró la ley modelo y Ecuador la internalizó mediante la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, R.O. 557 de 17-abril-2002, complementado con el reglamento,-diciembre-02-, constando en el capítulo II De las Infracciones Informáticas, artículos 57 en adelante, sancionando o penalizando a los mismos, reformaron a los artículos 202, 262, 353, 415, 553, 563, 606 #19º del Código Penal del Ecuador, que en la ley especial corresponde a los siguientes artículos: 58, 59, 60, 61, 62, 63 y 64. (Zambrano, 2012)

A continuación se listan las infracciones informáticas con su respectiva sanción:

Tabla 1.

Cuadro de infracciones a la seguridad de la información.

ART. 58: DELITOS CONTRA LA INFORMACIÓN PROTEGIDA (ART. 202 CP)	**SANCIÓN CARCELARIA**	**SANCIÓN PECUNIARIA**
Violentar claves o sistemas.	6 meses a 1 año.	$ 500 USD - $ 1000 USD
Información obtenida sobre la Seguridad Nacional, secretos comerciales o industriales.	3 años.	$ 1000 USD - $ 1500 USD
Divulgación o utilización fraudulenta de los rubros anteriores.	3 a 6 años.	$ 2000 USD - $ 10000 USD
Divulgación o utilización por funcionarios a cargo de dicha información.	6 a 9 años.	$ 2000 USD - $ 10000 USD
Obtención y uso no autorizado de datos personales para cederla o utilizarla.	2 meses a 2 años.	$ 1000 USD - $ 2000 USD
ART. 59: DESTRUCCIÓN MALICIOSA DE DOCUMENTOS POR FUNCIONARIOS DE SERVICIO PÚBLICO (ART. 262 CP.)	3 a 6 años	N/A
ART. 60: FALSIFICACIÓN ELECTRÓNICA SEGÚN EL SIGUIENTE DETALLE Y CON ÁNIMO DE LUCRO CON PERJUICIO A TERCEROS (ART. 535 CP.):		
Alterar un mensaje de datos. Simulación de un mensaje. Suposición de intervención en actos, declaraciones, etc.	6 años	N/A
ART. 61: DAÑOS INFORMÁTICOS (ART. 415 CP.) SEGÚN:		
Daño doloso de la información contenida en un sistema.	6 meses a 3 años.	$ 60 USD - $ 150 USD
Cometido por funcionario público o vinculado a la defensa nacional.	3 a 5 años.	$ 200 USD - $ 600 USD
Si no se tratare de un delito mayor, la destrucción, alteración e inutilización de infraestructura para la transmisión.	8 meses a 4 años.	$ 200 USD - $ 600 USD
ART. 62: APROPIACIÓN ILÍCITA (ART. 553 CP.) SEGÚN LO SIGUIENTE:		

Uso fraudulento o ilícito para apropiación de un bien ajeno, etc.	6 meses a 5 años.	$ 500 USD - $ 1000 USD
Uso fraudulento mediante la utilización de los siguientes medios: 1) Inutilización de sistemas de alarma. 2) Descubrimiento, descifrado de claves secretas o encriptados. 3) De tarjetas magnéticas, carding o perforadas. 4) de controles o instrumentos de apertura a distancia. 5) violación de seguridades electrónicas u otras semejantes.	1 a 5 años.	$ 1000 USD - $ 2000 USD
ART. 63: ESTAFA (ART. 363 CP.) A TRAVÉS DE MEDIOS ELECTRÓNICOS.	1 a 5 años.	$ 500 USD - $ 1000 USD
ART. 64: DERECHO A LA INTIMIDAD (ART. 606 #19 CP.) SI NO FUERE DELITO.	2 días a 4 días.	La sanción aún está en sucres equivalente a casi centavos.

Recuperado de: (Zambrano, 2012)

1.1.4. Riesgo de la información.

Los introducción de dispositivos BYOD incrementan las posibilidades de extraviarse y el robo de los dispositivos, así como el uso de redes inseguras como son las redes públicas, haciendo posible los ataques man in the middle[5]. El informe Norton 2013 de Symantec señala que en el año 2012, un 27% de los adultos reconocía haber perdido un dispositivo móvil o haber sufrido un robo del mismo. (Trend Micro, 2012) La pérdida de un dispositivo móvil no solo implica la fuga de información empresarial sino una pérdida de datos personales por parte del dueño de dicho dispositivo y que por consecuencia recae en la infracción al derecho inherente que tiene una persona a la privacidad. Este derecho se infringe cada vez que alguien intenta acceder a la información personal, de cualquier forma e independientemente de la plataforma, sin motivos legales o sin su consentimiento. De acuerdo con TrendMicro en su guía electrónica para la vida digital los ciberdelincuentes son conocidos infractores de la privacidad de los dispositivos móviles. Crean aplicaciones maliciosas como las de robo de datos, cuyo objetivo es conseguir información personal y financiera. Las aplicaciones gratuitas de alto riesgo también plantean varios problemas de privacidad, ya que compilan gran cantidad de información de tipología diversa.

De igual manera así como aumentan la productividad y eficacia existe la posibilidad de distracción por parte el empleado, dado las capacidades recreativas que estos dispositivos presentan (aplicaciones multimedia, acceso a redes sociales, mensajería instantánea y centros de entretenimiento y juegos). Adicionalmente hay que tener en cuenta que más de

[5] (CCN-CERT IA-21/13, 2013) **Man in the middle:** Es un ataque también llamado JANUS en el que el atacante adquiere la capacidad de leer y modificar los datos que se dan entre dos partes sin que ninguna de ellas se dé cuenta.

un tercio de las vulnerabilidades se derivan del uso de dispositivos BYOD puesto que pueden recaer en la transgresión de las normas de seguridad las empresas.

Varias investigaciones indican que casi el 75% (Trend Micro, 2012) de las organizaciones estudiadas permiten el acceso a información de las empresas a través de dispositivos que no están sujetos a la administración de seguridad corporativa y que, con frecuencia, la política de seguridad impartidas para tratar de mitigar esta problemática es ignorada por los empleados, cuyo conocimiento sobre los riesgos que se derivan por la fuga de información es mucho menor.

Acorde con María González Moreno, Asociada Senior de Información de ECIJA[6]: "En realidad, el utilizar dispositivos personales en el desarrollo de los puestos de trabajo no plantea riesgos adicionales a los ya existentes respecto del uso de portátiles o dispositivos de almacenamiento USB; riesgos de extravío o pérdida, de interceptación de las comunicaciones, fuga de información confidencial/corporativa, etc. Sin embargo, sí plantea posibles limitaciones en cuanto a la aplicación impositiva y restrictiva de las políticas de seguridad corporativas sobre dispositivos que no son propiedad de la organización y sobre los que ésta carece de control." Nos da un preámbulo a una de las principales problemáticas que plantea BYOD, lo cual es determinar la mejor forma para proteger físicamente dichos dispositivos, estableciendo reglamentos para designar responsables sobre el uso de cada dispositivo y como realizar un control lógico de acceso y conexión a los sistemas de las empresas mediante el monitoreo y gestión de detección de incidentes; logrando así documentar y mejorar continuamente los niveles de seguridad de las empresas.

1.2. ANÁLISIS COMPARATIVO Y REFERENCIAL GARTNER.

Para poder comprender de mejor manera un análisis de herramientas de seguridad de la información es importante considerar artículos, publicaciones e informes que comparen las funcionalidades que varias empresas presentan para solventar estas tendencias.

Uno de los informes más útiles que se puede encontrar a nivel de tecnología y emprendimientos de herramientas tecnológicas ha sido el Cuadrante Mágico del Grupo

[6] (Moreno, 2013) **ECIJA:** es la primera firma legal del mercado español en los sectores de TMT (Tecnología, Medios y Telecomunicaciones) y Propiedad Intelectual, de acuerdo con los principales rankings internacionales.

Gartner. Gartner, Inc. es una empresa de consultoría y de investigación en el mercado de las nuevas tecnologías. (Gartner, Inc., 2015)

El Cuadrante Mágico de Gartner es una representación gráfica de la situación del mercado de un producto tecnológico a lo largo de un periodo de tiempo establecido que generalmente suele estar dado por el periodo de un año. El grafico está dividido en cuatro partes o cuadrantes donde se distribuyen las principales características que las empresas mantienen en función a los productos que están presentando.

- *Leaders (líderes):* aquellas empresas que tengan la mayor puntuación resultante al combinar el soporte que mantienen en sus productos y servicios a nivel global y el alcance o la visión que pretenden con su producto.
- *Challengers (aspirantes):* están caracterizados por ofrecer buenas funcionalidades y mantener soporte en sus productos pero carecen de la visión global del producto.
- *Visionaries (visionarios):* se sitúan las empresas que pueden ofrecer todas las capacidades del producto en forma nativa o mediante alianza con otras empresas, logrando la integración de plataformas así como la habilidad de anticiparse a las necesidades del mercado que no logren cubrir.
- *Niche Players (nichos específicos):* son las empresas que están enfocadas en determinadas áreas de las tecnologías, sin mantener una solución completa que abarque completamente el área de análisis.

A continuación se muestra un ejemplo del cuadrante mágico de Gartner en una representación gráfica de la situación del mercado.

Figura 1. Reporte de Seguridad de la Información y Gestión de Eventos. Junio del 2014 *(Gartner, Inc, 2014)*

La consultora Gartner, indica en estudios recientes que el 36% de las empresas tienen una política de BYOD y un 32% tienen planificado la implementación de políticas de seguridad para integrar esta metodología en los próximos 12 meses. Considerando que en el año 2016, el 80% de los empleados optará por el uso de su propio equipo para laborar. (DeBeasi, 2011)

1.2.1. Niveles de Riesgo.

Uno de los mayores riesgos que implica el uso de dispositivos personales es la posibilidad que puedan usarse en distintas ubicaciones ya sean dentro de la infraestructura de las empresas como fuera de las mismas, lo cual facilita el acceso físico por parte de intrusos, tanto para la información personal que se almacena como para el acceso remoto a información crítica que se maneja, todo esto puede llevarse a cabo de la instalación de software de espionaje encubierto o malintencionado cuya función es extraer las credenciales de acceso de los usuarios a servicios web, mensajes de correo, información de llamadas de

telefonía y VoIp, agendas y contactos; para lograr mitigar estas falencias la gerencia de sistemas deberá implementar los siguientes niveles de seguridad:

Tabla 2.

Medidas de seguridad derivado de la movilidad.

Nivel 1: Exigiendo autenticación antes de lograr el acceso al dispositivo y/o a los recursos corporativos accesibles a través de dicho dispositivo. Tales mecanismos de autenticación suelen estar basados en contraseñas simples (PIN) y, salvo excepciones, asumiendo que el dispositivo en cuestión tiene un único usuario. Otros métodos de autenticación más robusta, tales como los basados en dispositivos externos (tokens), autenticación de dispositivos basada en red y autenticación de dominios. **Nivel 2:** No permitiendo el almacenamiento de información sensible en el dispositivo móvil. Si esto no es posible, será necesario proteger la información sensible almacenada Cifrándola, por ejemplo, haciendo al tiempo imposible su extracción del dispositivo por personas no autorizadas. **Nivel 3:** Proporcionando a los usuarios de dispositivos la formación y la concienciación necesarias para reducir los comportamientos poco seguros y su frecuencia.

Recuperado de: (CCN-CERT IA-21/13, 2013)

En cuanto al software o a los aplicativos instalados en los dispositivos se refiere, el principal riesgo es la incapacidad de detectar que tipo de software está instalado en los dispositivos personales que se conectan a la red y que pueden infectar nuestra red corporativa; en algunos casos los dispositivos móviles tienen acceso a tiendas ya sean oficiales y no oficiales de donde la descarga de contenido potencialmente peligroso es alta y de igual manera el acceso mediante códigos QR (Quick Response Codes)[7] los cuales pueden contener direcciones URL[8] a los que los dispositivos móviles acceden a través de sus cámaras haciendo imposible detectar si la URL destino da acceso a un sitio web peligroso;

[7] (Wave, 1994) **QR Code:** es un módulo que almacena información en una matriz de puntos o código de barras, cuya característica son tres cuadrados que se encuentran en las esquinas y permiten detectar la posición del código al lector.

[8] (Fundación Wikimedia, Inc., 2015) **URL:** es una cadena de caracteres con la cual se asigna una dirección única a cada uno de los recursos de información disponibles en la Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web

de igual manera sucede con dispositivos de escritorio o portátiles frente a lo que es phishing[9], aunque este último si se puede comprobar su legitimidad para así evitar su acceso de forma directa, para evitar el uso de los dispositivos, de sus aplicaciones y el ingreso a contenidos no confiables se sugiere tomar las siguientes medidas de seguridad:

Tabla 3.

Medida de seguridad de uso de dispositivos, aplicación y contenidos no confiables.

Nivel 1: Forzar el tráfico de datos a través de pasarelas web seguras y utilizar servidores proxy HTTP, u otros dispositivos intermedios para verificar las URL destino.
Nivel 2: Permitir la instalación de aplicaciones provenientes de "listas blancas" o facilitar el uso de las mismas en contenedores seguros (sandbox).
Nivel 3: Verificar que las aplicaciones tengan los permisos estrictamente necesarios para su adecuado funcionamiento.
Nivel 4: Prohibir el uso de ciertos dispositivos móviles o la instalación de aplicaciones de terceros (restringir su uso y acceso web).

Recuperado de: (CCN-CERT IA-21/13, 2013)

El uso de redes inseguras es otro riesgo que se debe afrontar para facilitar la interconexión de los dispositivos a los sistemas de información mediante el uso adecuado de protocolos de comunicación seguros evitando la intercepción de terceros y garantizando la interoperabilidad; para eso es recomendable seguir los siguientes niveles de seguridad:

[9] (CCN-CERT 401, 2014) **Phishing:** Son los ataques que usan la ingeniería social para adquirir fraudulentamente de los usuarios información personal (principalmente de acceso a servicios financieros). Para alcanzar al mayor número posible de víctimas e incrementar as sus posibilidades de éxito, utilizan el correo basura ("spam") para difundirse.

Tabla 4.

Medidas de seguridad para el uso de redes inseguras

Nivel 1: Usar mecanismos de cifrado fuerte (potenciar el uso de redes virtuales VPN).
Nivel 2: Usar mecanismos de doble autenticación o autenticación mutua que permitan a las partes involucradas en la comunicación identificarse mutuamente antes de intercambiar algún tipo de información.
Nivel 3: Prohibir el uso de redes inalámbricas inseguras, en especial aquellas en las cuales se han identificado vulnerabilidades.
Nivel 4: Desactivar las interfaces de red de los dispositivos que van a estar en desuso.

Recuperado de: (CCN-CERT IA-21/13, 2013)

Los dispositivos móviles continuamente comparten información a través de mecanismos inalámbricos, o por cable con el objetivo de sincronizar el contenido entre varios dispositivos ya sean equipos de escritorio o portátiles. Este riego ocurre cuando el usuario conecta el equipo móvil de su propiedad a un equipo de propiedad de la empresa o a cualquier equipo o estación no confiable como puede ser una estación de recarga, en el cual el almacenamiento de datos en ubicaciones no confiables puede recaer en el intercambio no autorizado de datos entre dispositivos o transmisión de código malicioso; para contrarrestar estos problemas se recomienda:

Tabla 5.

Medidas de seguridad para la interconexión con otros sistemas.

Nivel 1: Especificar qué dispositivos personales pueden sincronizarse con cuáles otros dispositivos de la organización.
Nivel 2: Prevenir que los usuarios puedan acceder a servicios de back-up remoto.

Recuperado de: (CCN-CERT IA-21/13, 2013)

1.3. DISEÑO DE APLICACIÓN DISTRIBUIDA.

Para poder entender que es una aplicación distribuida se tiene que comprender o desglosar algunos términos que son muy comunes en el desarrollo de software y que está asociado a la materia de ingeniería de software. En una aplicación distribuida se debe

comprender que son los componentes y que son los entornos de trabajo; como se distribuyen estos componentes y mediante que mecanismo se comunican los mismos.

Una distribución se comprende como la construcción de un software por componentes que están relacionados a funciones específicas. Cada uno de estos componentes pueden estar separados de manera física conocida como “Niveles” (layers) o de manera lógica también conocida como “Capas” (tiers) (Garcia, 2009). Esta distribución no se la toma de manera arbitraria sino que está relacionada con las consideraciones técnicas como son el escenario y el tipo de aplicación que se va a desarrollar, la lógica del negocio y la interoperabilidad de los componentes. Hay que tener en cuenta que una capa puede contener varios componentes y a su vez un componente puede estar distribuido en varias capas todo acorde a la lógica el negocio o a factores económicos que el arquitecto de la aplicación determine necesaria.

Un componente es un elemento de software que contiene embebido un conjunto de funciones todas estas encapsuladas acorde al lenguaje de programación orientada a objetos y que puede ser utilizado en conjunto con otros componentes interactuando para formar un sistemas más complejos. Cada componente está formado por clases o recursos que están regidos por los principios básicos de la programación orientada a objetos:

- *Modularidad:* es la propiedad que permite crear una aplicación en base a partes reducidas, componentes o módulos; cada una de las cuales debe ser independiente y permitir la interconexión con otros.
- *Reusabilidad:* debido a que las aplicaciones están típicamente compuestas por partes similares, la mayoría del software nuevo puede ser ensamblado a partir de componentes preexistentes.

Los componentes de igual manera que los objetos tiene que cumplir con dos características importantes:

- *Alta Cohesión:* es cuando todos los elementos internos dentro de un componente están estrechamente relacionados.
- *Bajo Acoplamiento:* hace referencia cuando sus modulo sestan desarrollados de tal forma que permiten mayor escalabilidad, evitando dependencias intrínsecas.

Figura 2. Componentes de una aplicación distribuida. *(Garcia, 2009)*

Una aplicación distribuida es aquella cuyo principal objetivo es alcanzar mediante la ejecución de varios procesos independientes o modulares que por lo general se ejecutan en diferentes niveles o capas que se interconectan y pasan datos entre ellos. Las características principales de una aplicación distribuida son:

- *Concurrencia:* De igual forma que en las aplicaciones centralizadas, las aplicaciones distribuidas serán utilizadas por cierto número de usuarios concurrentemente.
- *Topología de la red:* A pesar de que a día de hoy los anchos de banda cada vez son más amplios, el tráfico de red puede ser un aspecto importante que condicione el tiempo de respuesta de la aplicación.
- *Ubicación de la lógica:* Dado que en una aplicación distribuida intervienen varios procesos, será necesario decidir en cuál de los posibles procesos físicos se sitúa cada componente lógico de la aplicación.
- *Homogeneidad de las plataformas:* En una aplicación distribuida los sistemas operativos involucrados o los lenguajes de desarrollo utilizados pueden ser un factor a tener en cuenta a la hora de decidir algunos aspectos importantes.
- *Seguridad:* Una aplicación distribuida mantiene procesos que de una forma u otra están a la escucha en una red, lo que aumenta la vulnerabilidad de la aplicación. (Preciado, 2015)

1.3.1. Entorno Cliente - Servidor.

El modelo cliente - servidor es un modelo de informática centralizada en la cual los usuarios trabajan en computadores denominados clientes o sistemas frontales (front-end) e interaccionan o intercambian información con los sistemas en los servidores denominados posteriores o (back-end), los mismos que están encargados de proporcionar servicios, control de accesos, gestión de red y almacenamiento centralizados. El modelo cliente-servidor se aplica en sistemas operativos, aplicaciones, gestión de bases de datos, entre otros. Los sistemas operativos de red están orientados a este modelo ya que los usuarios situados en las estaciones de trabajo realizan peticiones a los servidores un claro ejemplo es el sistema operativo de red Netware perteneciente a Novell. El cliente ejecuta un programa que re direcciona las peticiones de obtención de los servicios de la red al servidor adecuado, además de enviar las peticiones de servicios locales al sistema operativo local. En los sistemas gestores de bases de datos que siguen el modelo cliente-servidor, los clientes realizan las consultas a través de una aplicación frontal que atienden los servidores.

"Los servidores en un entorno cliente-servidor son equipos robustos centrales, capaces de gestionar adecuadamente las múltiples y simultáneas peticiones que reciben de los clientes, además de realizar tareas de seguridad y gestión de red. Algunas organizaciones han reemplazado sus computadoras centrales, que proporcionaban cinco millones de instrucciones por segundo (MIPS)[10], por un grupo de servidores capaces de ejecutar 1.000 MIPS. Las diversas estrategias cliente-servidor ofrecen una forma de crear plataformas informáticas relativamente asequibles y fáciles de configurar según las necesidades específicas de las aplicaciones." (Osorio, 2001)

1.3.2. Arquitectura.

La arquitectura cliente-servidor es un modelo de aplicación distribuida en el que las tareas se reparten entre los servidores o proveedores de servicio y las estaciones de trabajo llamadas clientes. La arquitectura cliente-servidor define una relación entre el usuario de una estación de trabajo y un servidor posterior de archivos, impresión, comunicaciones u otro tipo de sistema proveedor de servicios. El cliente debe ser un sistema inteligente con su

[10] (Osorio, 2001) **MIPS:** Es la cantidad de instrucciones por segundo que recibe un procesador, mediante la cual se puede medir la potencia de un procesador; siendo esta medida útil cuando se comprara procesadores con la misma arquitectura.

propia capacidad de procesamiento para descargar en parte al sistema posterior siendo ésta la base del modelo cliente – servidor.

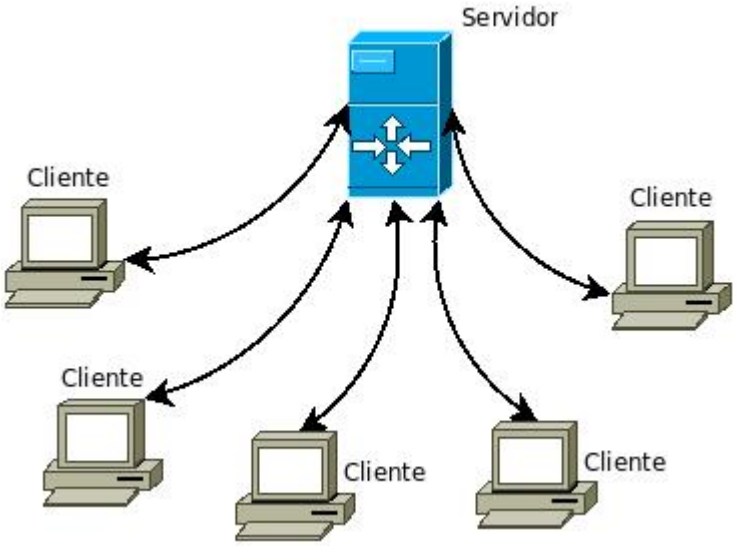

Figura 3. Modelo cliente - servidor. *(CATEDU, 2015)*

En la arquitectura cliente – servidor, el servidor debe negociar y gestionar con su sistema operativo un puerto que debe ser conocido y va de acuerdo al servicio que ofrece y es mediante el cual resuelve las peticiones que genera el cliente. Para gestionar las peticiones el servidor se encuentra en espera la misma que se realiza de manera pasiva hasta que llega la solicitud enviada por el cliente y el servidor está en la capacidad de manejar todas las peticiones concurrentes, así como despliega los procedimientos de acceso y protección del sistema. “Desde un punto de vista funcional el modelo cliente – servidor está definido como una arquitectura distribuida” (Preciado, 2015) que permite asignar los procesos y los datos de forma eficiente admitiendo a los usuarios finales tener acceso a la información mediante el uso de solicitudes de manera transparente en entornos multiplataforma.

Actualmente existen variantes a la implementación del modelo cliente – servidor, teniendo como la configuración más común en la que varios clientes se interconectan y acceden a un solo servidor central. Otro modelo convencional es la de servidores distribuidos en donde las estaciones de trabajo (clientes) acceden a la base de datos que se encuentra en varios servidores. De igual manera en los entornos de red en los que los clientes están a la par, gestionados en grupos de trabajo como son el caso de Windows, la compartición de archivos se convierte en un modelo de cliente – servidor donde cada estación de trabajo

puede desempeñar la función de servidor ya que comparte ciertos archivos a otra estación de trabajo proporcionando una configuración cliente – servidor entre pares. (Osorio, 2001)

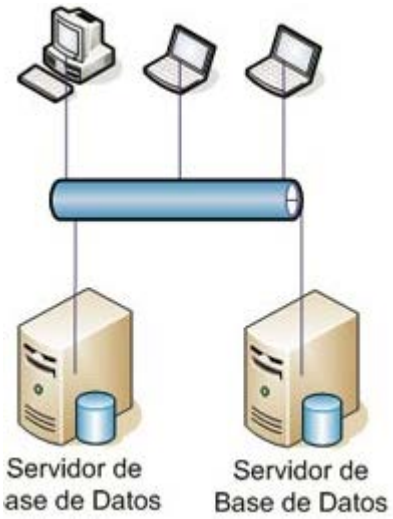

Figura 4. Configuración cliente - servidor con servidores distribuidos. *(Vásquez Villacreses, 2015)*

Por lo general, el cliente y el servidor dependen de la configuración del entorno o de la lógica del negocio por lo cual los procesos que manejan están determinados por las herramientas de redirección que tienen los clientes ya sea para balancear la carga de trabajo, administrar la carga de procesamiento o gestionar las seguridades de la empresa.

En la mayoría de las configuraciones la interoperabilidad y comunicación se realiza mediante la red[11] en donde los servidores pueden ser parte de un grupo de trabajo y estar ubicados físicamente en una zona centralizada de la empresa; o también pueden estar ubicados remotamente en donde los usuarios deben acceder mediante un enlace de telecomunicaciones y que acorde con el tipo de conexión y de las restricciones de seguridad diseñadas las peticiones pueden tener respuestas de segundos, minutos u horas.

1.3.3. Funcionalidades.

El modelo cliente – servidor tiene algunos beneficios que ayudan a las empresas a manejar la interoperabilidad y brinda una escalabilidad ya que permite redimensionar a partir de ordenadores centrales hacia servidores y estaciones de trabajo sobre la red constituyendo una plataforma corporativa. Las principales ventajas que presenta este modelo son:

[11] (Kioskea, 2015) **Red:** Una red informática está compuesta por varios equipos que están interconectados entre sí mediante líneas de comunicación y elementos de hardware que garantizan que los datos viajen correctamente y que varían según su tamaño, velocidad y alcance.

- "*Recursos centralizados:* debido a que el servidor es el centro de la red, puede administrar los recursos que son comunes a todos los usuarios, por ejemplo: una base de datos centralizada se utilizaría para evitar problemas provocados por datos contradictorios y redundantes.
- *Seguridad mejorada:* ya que la cantidad de puntos de entrada que permite el acceso a los datos no es importante.
- *Administración al nivel del servidor:* ya que los clientes no juegan un papel importante en este modelo, requieren menos administración.
- *Red escalable:* gracias a esta arquitectura, es posible quitar o agregar clientes sin afectar el funcionamiento de la red y sin la necesidad de realizar mayores modificaciones." (Kioskea, 2014)

Algunas funcionalidades que presenta este modelo es el desarrollo de aplicaciones en n-capas separando los componentes de una aplicación en capas lógicas y/o físicas dando origen a varios modelos de distribuciones de aplicaciones logrando incluir multiplataforma, bases de datos, redes y sistemas operativos; los mismos que puedes ser arquitecturas propietarias y no propietarias pero todas interconectadas y funcionando al mismo tiempo.

CAPÍTULO 2. SEGURIDAD DE LA INFORMACIÓN

2.1. INTRODUCCIÓN

Debido al incremento del uso de las telecomunicaciones, el cual permite a los empleados conectarse a los sistemas de información desde cualquier lugar las empresas en la actualidad son víctimas de varias amenazas lo cual representa pérdidas de miles o millones en sus activos; por tal motivo es necesario revisar cuales son las herramientas que se encuentran disponibles en nuestro medio, que sistemas se pueden implementar para mitigar la perdida de información y que modelos de ambientes pueden coexistir con la tendencia BYOD que se analizó anteriormente.

Por lo general, los sistemas de seguridad de información son herramientas que se deben integrar al giro de negocio de la empresa para garantizar la integridad, confidencialidad y disponibilidad de la información; las mismas que se pueden encontrar bajo varios tipos de licenciamiento y modelos de implementación.

Durante este capítulo se analizara soluciones de seguridad comerciales cuyo modelo de implementación es en la nube, lo cual aplica a las empresas que no disponen de la infraestructura necesaria y las aplicaciones “on premise” o en las instalaciones las cuales requieren una infraestructura ya arquitectura especializada para su correcto despliegue y funcionamiento.

2.2. HERRAMIENTAS DE SEGURIDAD DE LA INFORMACIÓN.

El incremento del uso del internet ha desarrollado un aumento en la interconectividad y la interoperabilidad que tienen las compañías con sus socios haciendo importante conocer que recursos de la compañía necesitan ser protegidos mediante el control de acceso a sus sistemas y mitigar los riesgos de fuga de la información. Acorde con la Organización Internacional de Normalización (ISO) fue publicado y aprobado en octubre del 2005 en conjunto con la Comisión Electrónica Internacional (IEC) la definición de seguridad informática:

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio”. (ISO/IEC, s.f.)

Al valorar la seguridad de la información en una empresa se debe plantear un sistema que nos permita preservar la confidencialidad, la integridad y la disponibilidad de dicha información con lo cual todo sistema de seguridad debe cumplir con cinco objetivos principales:

- *Integridad:* garantizar que los datos sean los que se supone que son.
- *Confidencialidad:* asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- *Disponibilidad:* garantizar el correcto funcionamiento de los sistemas de información.
- *Evitar el rechazo:* garantizar de que no pueda negar una operación realizada.
- *Autenticación:* asegurar que sólo los individuos autorizados tengan acceso a los recursos. (ISO 27000.es, 2005)

2.3. SISTEMAS DE SEGURIDAD DE DISPOSITIVOS FINALES.

En el capítulo dos que hace referencia a la comunicación a través de la red de la guía de estudio para CCNA Exploration 4.0, se puede encontrar una clasificación de los dispositivos, elementos o equipos que intervienen en una red, clasificados en dispositivos intermedios y dispositivos finales.

"Los dispositivos finales son aquellos que constituyen la interfaz entre la red humana y la red de comunicación subyacente, como por ejemplo:

- Computadoras (ordenadores, portátiles, servidores Web).
- Impresoras de red.
- Teléfonos VoIP.
- Cámaras de seguridad.
- Dispositivos móviles de mano (PDA)." (Cisco, 2008, pág. 45)

A su vez, los dispositivos finales se clasifican en dispositivos cliente y dispositivos servidor:

- *Clientes:* son hosts que tienen software instalado que les permite solicitar o mostrar la información obtenida del servidor.
- *Servidores:* son hosts que tienen software instalado que les permite proporcionar información y servicios (emails, páginas web, etc). (Cisco, 2008, págs. 45, 46)

Los dispositivos intermediarios proporcionan conectividad entre redes y administran los flujos de datos por la red. Los dispositivos intermediarios se clasifican en dispositivos:

- *Dispositivos de Red:* (hub, switches y puntos de acceso inalámbricos).
- *Dispositivos Internetworking* (router).
- *Dispositivos de comunicación* (modems).
- *Dispositivos de seguridad* (firewalls). (Cisco, 2008, pág. 46)

Los procesos que ejecutan los dispositivos intermediarios de red son los siguientes:

- Regeneran y retransmiten señales.
- Mantienen información sobre rutas y destinos a través de la red.
- Sistemas de detección de errores y pérdidas en las comunicaciones.
- Cálculo y redirección de rutas alternativas.
- Prioridades de QoS[12](calidad de servicio).
- Configuraciones de seguridad. (Cisco, 2008)

Los sistemas de seguridad en la actualidad ofrecen soluciones más robustas que un simple aplicativo de detección de software mal intencionado, deben contemplar un conjunto de aplicaciones que permitan una seguridad sólida, rápida y sencilla de implementar, protegiendo los diferentes sistemas operativos que hoy en día se manejan: Windows, Linux y Mac sin descuidar los dispositivos móviles como son los smartphones y tablets, Android e iOs. Bajo este esquema una herramienta de seguridad debe permitir gestionar los diferentes ambientes que las empresas manejan centralizando su uso.

2.3.1. MDM (Mobile device management).

Es un modelo de aplicación que permite asegurar, monitorear y gestionar los dispositivos móviles así como sus datos la información que acceden y manejan para presentar resultados. De igual manera la mayor parte de las plataformas de gestión de dispositivos móviles permiten la localización, rastreo y administración de aplicaciones de forma remota. Esta solución es una de las más usadas por las empresas debido a su alta

[12] (Wikipedia, 2009) **QoS:** "es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red. Cuantitativamente medir la calidad de servicio son considerados varios aspectos del servicio de red, tales como tasas de errores, ancho de banda, rendimiento, retraso en la transmisión y disponibilidad"

escalabilidad ya que representa la primera defensa para hacer frente a la tendencia "BYOD" en cuanto a la seguridad de la información se refiere.

La intención de la implementación de un MDM es optimizar la funcionalidad y la seguridad de los dispositivos móviles dentro de la empresa, al mismo tiempo que brinda protección al acceso a la red corporativa. Una de las características más importantes en la elección de un MDM debe ser la compatibilidad con las diferentes plataformas operativas que los dispositivos móviles presentan, de igual manera la transmisión de los datos lo hacen de manera de múltiples proveedores de servicios.

En el esquema básico un MDM está conformado por un agente, que es una aplicación que se encuentra en cada uno de los dispositivos móviles que se desea administrar, es una aplicación cliente que mantiene una conexión con el servidor a través de una red de telecomunicación sea por Wi-Fi[13], GPRS[14], 3G[15], 4G o cualquier otro medio de transmisión de datos sin tomar en cuenta el proveedor del servicio.

Algunas de las funcionalidades más destacadas en los MDM en el mercado son:

- *Instalación masiva de aplicaciones:* se pueden instalar aplicaciones, ejecutar actualizaciones y administrar parches de seguridad en múltiples dispositivos, de forma remota.
- *Selección de aplicaciones:* esta funcionalidad permiten aplicar políticas de control sobre las aplicaciones que los dispositivos pueden correr, de esta manera se evita que los usuarios ejecuten aplicaciones que no son productivas para las empresas determinando los tiempos de ejecución.
- *Rastreo satelital:* gracias al uso de GPS, se puede localizar la ubicación de uno o más dispositivos así como hacer un rastreo de la ruta que mantuvieron durante un período dado.
- *Sincronización de Archivos:* se pueden mantener los archivos de los dispositivos sincronizados con el servidor y mantener las últimas versiones en los dispositivos facilitando la colaboración entre empleados.

[13] (Wikipedia, 2014) **Wi-Fi:** Es el mecanismo de conexión de dispositivos electrónicos de manera inalámbrica.
[14] (Wikipedia, 2015) **GPRS:** Es la transmisión de datos mediante la conmutación de paquetes.
[15] (Informatica Hoy, 2012) **3G:** Es una tecnología móvil que permite la transmisión de voz y de datos a través de telefonía móvil mediante el servicio universal de telecomunicaciones móviles (UMTS).

- *Bloqueo de funciones:* un MDM permite controlar funciones específicas de los dispositivos pudiendo activar o desactivar la cámara, micrófono, USB, acceso a configuración de dispositivo, entre otros.
- *Borrado remoto:* es una función imprescindible, que se usa cuando el dispositivo móvil está extraviado, robado o perdido y se desea prevenir la fuga de datos que residen en el mismo.
- *Bloqueo por contraseña:* desde el servidor, se puede establecer una contraseña de bloqueo y también se puede configurar la longitud, el tipo de contraseña, para tener acceso al dispositivo.

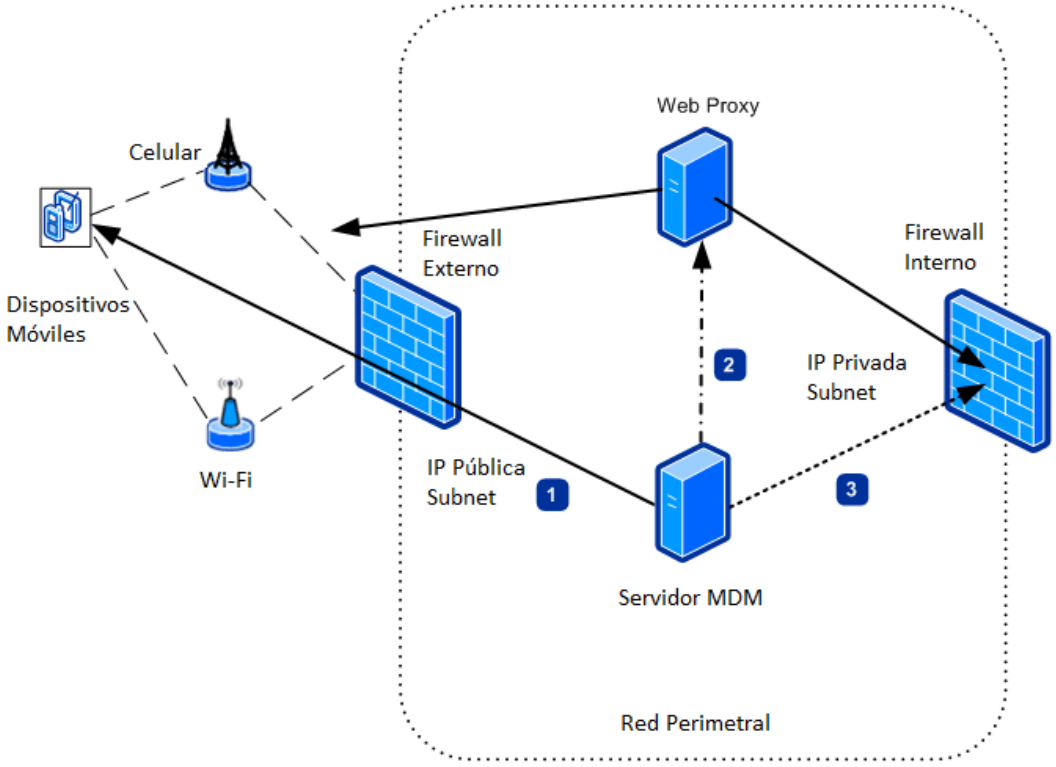

Figura 5. Configuración de la red perimetral MDM *(Microsoft, 2009)*

2.3.2. SEM (Security Endpoint Manager).

Es una herramienta de software diseñada para facilitar la gestión de los recursos de TI, con lo cual se busca administrar los servicios y gestionar las políticas de seguridad de los dispositivos finales en las empresas como son los ordenadores, laptops y que permite la escalabilidad mediante la administración de dispositivos móviles. La principal función de estas herramientas es mantener los dispositivos y aplicaciones en perfecto estado manteniendo la productividad del personal.

El control de las aplicaciones reduce la exposición de los equipos a los ataques evitando que ejecuten software desconocido o no deseado acoplando la infraestructura a políticas flexibles que se pueden gestionar mediante el usos de listas blancas y listas negras, de igual manera algunas soluciones permiten el análisis mediante la interconexión con bases de datos de aplicaciones a nivel mundial mediante la interoperabilidad en la nube y compartición de datos estadísticos entre varios usuarios.

En su arquitectura un SEM está conformado por un cliente que se encuentra instalado en los dispositivos finales o endpoint, el cual se encarga de la protección contra malware, virus, spyware de forma continua permitiendo establecer control de accesos y centralizando la gestión de todos los equipos de las empresas en una sola consola ahorrando tiempo en las tareas de implementación y a la vez manteniendo la privacidad de los datos críticos de la empresa.

En relación al análisis de prestaciones, algunas de las características más destacadas de estas herramientas se listan a continuación:

- *Protección integral y completa:* la gran parte de los sistemas de seguridad de información utilizan técnicas de última tecnología para brindar la mayor protección contra malware.
- *Control de intrusión:* los sistemas contra intrusión emplean sistemas de prevención basados en el host (HIPS)[16] ofreciendo protección a tiempo real frente a los ataques maliciosos ya sean conocidos o desconocidos impidiendo la ejecución e instalación de software desconocido e indeseado.
- *Gestión centralizada:* la mayor parte de las funciones de supervisión, control y prevención de los equipos se lo realiza en una sola consola la cual puede ser gestionada remotamente.
- *Implementación fácil:* la instalación de la plataforma tanto en servidores como en las estaciones de trabajo se lo realiza de forma intuitiva ahorrando tiempo de implementación, de igual manera la integración por la red facilita la gestión y despliegue de políticas de seguridad, mediante el uso de plantillas predeterminadas.

[16] (Arntz, 2013) **HIPS:** son los sistemas de prevención de intrusiones que monitorean la actividad del sistema y emplea un conjunto de reglas predefinidas para detectar el comportamiento sospechoso de una aplicación o del sistema en general.

- *Privacidad:* las herramientas facilitan la creación de un entorno virtual privado y aislado en las estaciones de trabajo, asegurando la confidencialidad de los datos empresariales, en algunas herramientas se puede anexar módulos para la prevención de fuga de información conocida en el mercado como herramientas de DLP[17].
- *Solución escalable:* gran parte de las soluciones de gestión de seguridad de la información permiten la implementación remota y se integran con sistemas ya puestos en producción como son los sistemas de correo electrónico y compartición de archivos permitiendo el crecimiento de las empresas y la compatibilidad entre varias soluciones pre existentes permitiendo adaptarse a las necesidades y presupuestos del negocio.
- *Sistemas de gestión:* la solución comprende un conjunto de herramientas que permite optimizar tiempos de actualización de aplicaciones mediante el envío centralizado de paquetes o parches de actualización a los dispositivos finales, adicionalmente algunas herramientas integran la búsqueda por red facilitando la generación de informes de inventarios de software y de hardware y gestión de licencias.

Las funcionalidades permiten desplegar una plataforma robusta de seguridad de la información que se puede integrar a servicios de autenticación ya sea un directorio activo o cualquier administrador de dominio logrando tener un control más adecuado de la información mediante la distribución centralizada de políticas de seguridad y encriptación facilitando el uso de los dispositivos finales en cualquier área de trabajo ya sea dentro de la empresa o fuera de ella.

[17] (Symantec, 2015) **DLP:** (Data Loss Prevention) son los sistemas que permiten la detección, supervisión y administración de los datos confidenciales de una empresa en donde sea que se encuentren y utilicen.

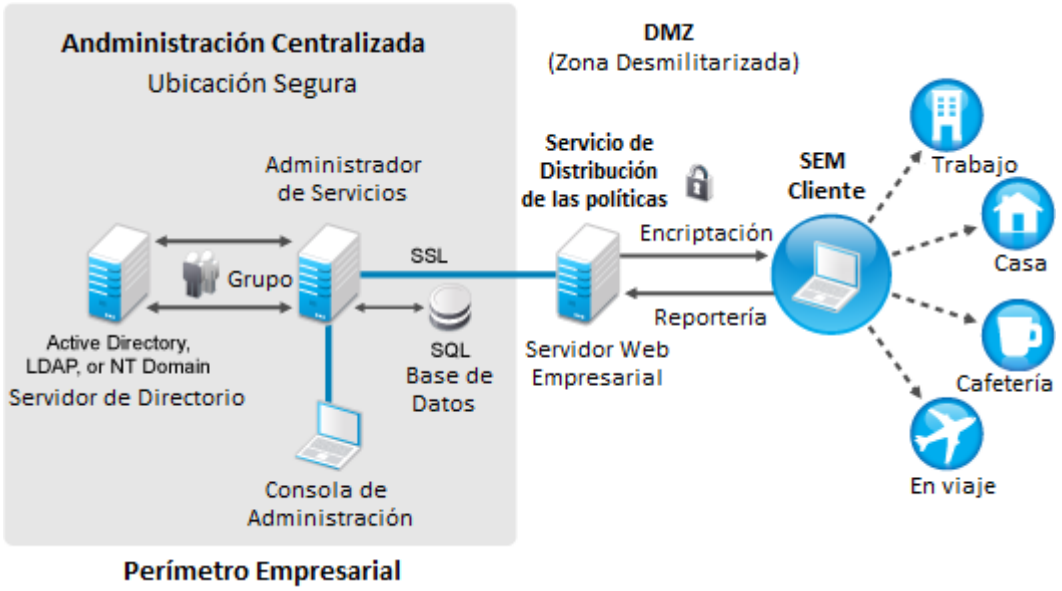

Figura 6. Arquitectura de Security Endpoint Manager – Caso particular ZENWorks SEM *(Novell, 2015)*

2.3.3. Sistemas Basados en la Nube (SaaS).

Es un modelo de negocio considerado como una experiencia del usuario en la cual se ofrecen recursos de TI, ya sean aplicaciones, datos y parte de la infraestructura como un servicio. Generalmente los activos involucrados no están centrados en una misma ubicación física dando ventajas como:

- *Abstracción:* El usuario se desentiende de los detalles técnicos.
- *Elasticidad:* Permite a la empresa escalar la infraestructura en pocos pasos.
- *Aprovisionamiento:* Recibir y liberar recursos de acuerdo a las necesidades de la empresa.
- *Virtualización:* Se puede tener varias máquinas virtuales en un solo servidor físico disminuyendo los costos de infraestructura considerablemente.
- *Facturación por Recurso y por uso:* El licenciamiento es más simple y se lo hace acorde a las necesidades de la empresa. (The Open Group, 2011)

SaaS busca estructurar los procesos de negocio como componentes reutilizables e intercambiables. Es una tecnología que se debe adaptar al negocio, no al revés en la cual se ofrece las aplicaciones como un servicio donde el usuario no debe preocuparse por el mantenimiento ya sean estos parches de seguridad, actualizaciones de las aplicaciones. Un claro ejemplo de SaaS o una categoría más común son:

- CRM[18] o Customer Raltionship Management.
- Correo electrónico empresarial / personal. (Darnalt C. , 2013)
- Compartición de archivos.

SaaS es un modelo de computación en la nube y está relacionado con SOA que es la Arquitectura Orientada al Servicio de tipo "black-box" [19] que nos permite alcanzar flexibilidad y abstracción mediante el aprovisionamiento de soluciones dedicadas.

Algunas desventajas de usar este modelo es que los usuarios no disponen un acceso directo a sus contenidos ya que están almacenados en equipos externos a las empresas, a menos que la plataforma permita la exportación de los datos con lo cual se debe contar con mecanismos de control de acceso a la información mediante el uso de cifrado y doble autenticación de usuarios.

Si la empresa que contrato la plataforma de seguridad no dispone del servicio de internet por parte del ISP[20], el acceso a la información será nula, por lo que su operatividad estará sujeta a las medidas de contingencia que tenga para prever dichas amenazas y asegurar la continuidad del negocio.

[18] (Darnalt C. , 2013) **CRM:** Es una estrategia para la gestión de las relaciones e interacciones que se mantienen entre la empresa y sus clientes y clientes potenciales. (Salesforce.com EMEA Limited, 2000 - 2015)
[19] (Cross Check Networks, 2005- 2013) **Black Box:** Es una metodología desarrollada para el despliegue de forma robusta, escalable, interoperable y segura de Servicios Web.
[20] (Wikipedia, 2014) **ISP:** es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cable módem, GSM, dial-up, fibra óptica, etc.

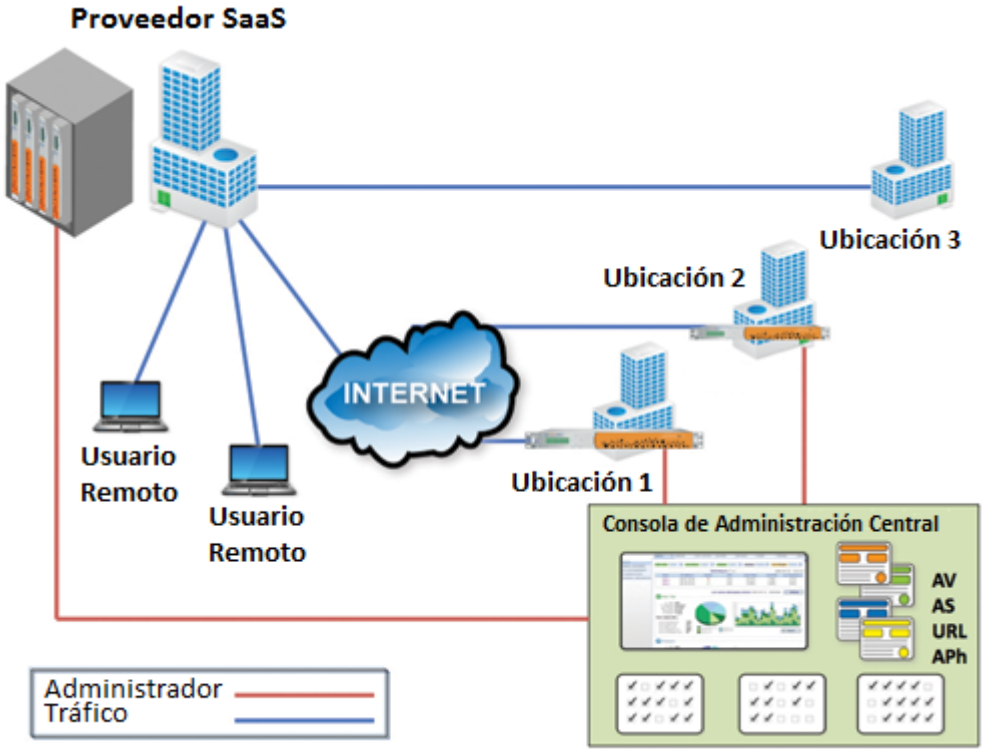

Figura 7. Arquitectura Básica de Sistemas en la Nube (SaaS). *(Optenet, 2015) (Vásquez Villacreses, 2015)*

Otras modalidades para distribución de software son:

- *Plataform-as-a-Service (PaaS):* es el modelo de computación en la nube que provee un conjunto de soluciones dedicadas a desarrollar e implementar aplicaciones propias como son autenticación, mensajería entre otras. En este modelo la infraestructura nos la da la plataforma. Es un modelo que reduce la complejidad al desplegar y mantener aplicaciones ya que las soluciones PaaS gestionan automáticamente la escalabilidad usando más recursos si fuera necesario. Ofrecen facilidades para cubrir todas las etapas que comprenden el desarrollo de una aplicación pero todo ello sin entrar al nivel de máquinas.
- *Infraestructure-as-a-Service (IaaS):* en este modelo computacional con IaaS existe un mayor control que con PaaS, mediante el cual se tiene el control de la gestión de infraestructura, en el cual se renta o alquila por un determinado tiempo la infraestrcutura de IT. Durante este proceso ambas partes acuerdan un nivel de servicio bajos los criterios de disponibilidad (uptime), tiempos de recuperación frente a desastres, provisión automática de recursos acorde a la necesidad, entre otros. La empresa que contrata el servicio puede elegir qué

tipo de instancias desea usar Linux o Windows, así como la capacidad de memoria o procesador de cada una de las máquinas (servidores). El hardware para este modelo es transparente, puesto que todo lo que se maneja es de forma virtual en al cual cada clientes es el encargado de escalar las aplicaciones según sus necesidades, además de preparar todo el entorno en las máquinas.

2.4. HERRAMIENTAS SaaS.

Son un modelo de distribución de software donde el soporte lógico y datos que maneja la empresa se alojan en servidores externos, a los cuales se tiene acceso mediante la red, en donde la empresa proveedora de este servicio se ocupa del mantenimiento y operación diaria así como el soporte del software y plataforma que usa el cliente.

2.4.1. Citrix XenMobile.

Es una completa plataforma que integra la administración de dispositivos móviles (MDM) con la gestión de aplicaciones móviles (MAM) para mantener la seguridad y las necesidades de conformidad de las gerencias TI.

“XenMobile es una solución de software MDM líder del sector que admite todas las principales plataformas móviles, lo que hace fácil que TI administre y configure dispositivos durante todo su ciclo de vida y proporcione a los usuarios la flexibilidad para trabajar en cualquier dispositivo que elijan.” (Citrix, 2014)

La plataforma de XenMobile permite la administración de movilidad empresarial basada en la nube, la misma que se denomina XenMobile Cloud; la cual combina todas las capacidades de administración de datos, aplicaciones y dispositivos móviles con la flexibilidad, facilidad de administración con un menor costo total de propiedad en la nube. Estos servicios se encuentran alojados en centros de datos seguros en todo el mundo, XenMobile Cloud se encuentra administrado por un equipo dedicado de ingeniería en la nube en Citrix. El equipo de nube administra todas las actualizaciones y mantenimiento de XenMobile, de forma que puede trabajar en proyectos críticos para la empresa en su organización en vez de dedicarse a estas tareas facilitando y reduciendo los costos de infraestructura en las empresas.

La integración de XenMobile es uniforme garantizando controles de seguridad y experiencia del usuario fluida. Referente a seguridad de la información la herramienta tiene tres pilares de seguridad:

- Conformidad con FIPS[21] multiplataforma para entornos de BYOD y dispositivos mezclados.
- Validación y comprobación de penetración de terceros.
- Conformidad con SOC 1/SSAE 16 y ISO27001 para la oferta de nube de XenMobile.

Citrix presenta su solución como un administrador de dispositivos móviles basada en roles, y complementándola con la gestión de aplicaciones permitiendo inclusive detectar si los equipos están haciendo uso de root o jailbreak fuera del cumplimiento de las políticas de seguridad logrando una solución integral para la gestión de dispositivos móviles, aplicaciones, y los datos mientras que da a los usuarios la libertad de experimentar el trabajo a su manera. La arquitectura móvil de la solución incluye:

- Configurar, proteger, el suministro y apoyar los dispositivos móviles con MDM.
- Gestión de aplicaciones móviles con la mayor integración de aplicaciones para las empresas.
- Aplicaciones de correo electrónico de espacio aislado (SandBox), navegador y colaboración del trabajo mediante la compartición de documentos.
- Tienda de aplicaciones corporativas unificada.
- Inicio de sesión único por autenticación de multifactor.

De igual manera Citrix integra la herramienta Worx Home que permite a la gerencia de IT hacer cumplir las configuraciones móviles y la seguridad mientras proporciona el acceso a una tienda de aplicaciones unificadas para entregar políticas de seguridad específica y política de aplicaciones habilitadas para Worx. El acceso a los datos está controlado por NetScaler Gateway el mismo que proporciona a los administradores un control granular a nivel de los datos y fortalece el soporte a los usuarios con acceso remoto desde cualquier

[21] (Wikipedia, 2013) **FIPS:** son los estándares anunciados públicamente y desarrollados para el procesamiento de la información.

lugar; ofreciendo un único punto para gestionar las acciones de control de acceso y limites dentro de las sesiones basadas en las credenciales de los usuarios.

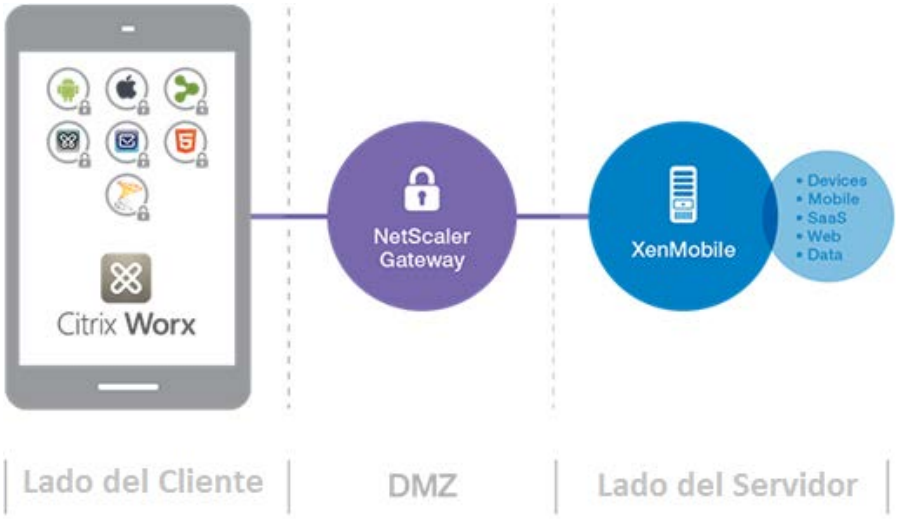

Figura 8. Administración de movilidad Empresarial. *(Citrix, 2014)*

Los administradores pueden aprovechar la información almacenada de los flujos de trabajo para definir reglas basadas en nombre de usuario, cargo o función y establecer un orden de aprobación y de ser necesario un número determinado de aprobaciones para la delegación de tareas.

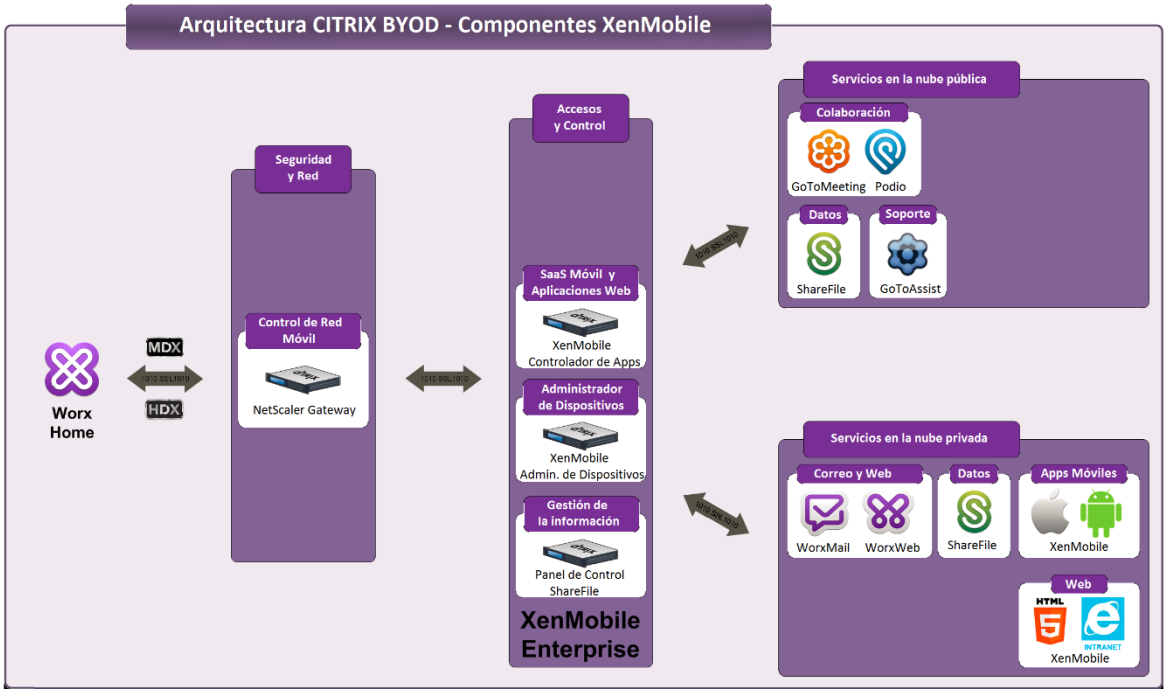

Figura 9. Arquitectura Citrix BYOD con XenMobile *(Citrix, 2014)*

Citrix XenMobile ofrece una solución completa para la gestión de aplicaciones, datos y dispositivos que se acopla al mercado con toda la gama de soluciones que ofrece.

Tabla 6.

Funciones disponibles de las soluciones de XenMobile

FUNCIONES	XenMobile MDM	XenMobile App	XenMobile Enterprise
Configurar, asegurar y provisionar dispositivos móviles.	✓		✓
Soporte y Chat en vivo con un clic.	✓		✓
Acceso a unidades der y SharePoint.	✓	✓	✓
Navegador web móvil seguro.	✓	✓	✓
Aplicaciones específicas micro VPN.		✓	✓
Correo seguro, calendario y contactos.		✓	✓
Habilitar cualquier aplicación móvil empresarial.		✓	✓
Integración similar a las aplicaciones Windows.		✓	✓
Tienda de aplicaciones corporativas unificadas.		✓	✓
Inicio de sesión único por autenticación de multifactor.		✓	✓
Compartición de documentos seguro, sincronización y edición.			✓
Opciones de almacenamiento de datos tanto en la nube como en las instalaciones.			✓

Recuperado de: (Citrix, 2014)

2.4.2. MaaS360[22].

Es la plataforma de gestión de la movilidad basada en la nube más robusta que se extiende a través de dispositivos, usuarios, aplicaciones, documentos y gastos de infraestructura como son licenciamiento y actualizaciones de seguridad.

MaaS360 Secure Productivity Suite ofrece un conjunto completo de soluciones multiplataforma para aislar y contener los datos de trabajo frente a la tendencia BYOD. Es una solución completa basada en la nube para los teléfonos inteligentes y tabletas que permite a los empleados acceder de forma segura a los datos corporativos mientras que

[22] **ACLARACIÓN:** Durante el desarrollo de la presente disertación la herramienta **MaaS360** pertenecía a la compañía **FiberLink Communications** que posteriormente fue adquirida por **IBM**. En la actualidad **MaaS360** es una compañía que pertenece a **IBM**.

preserva la experiencia móvil en sus dispositivos personales; adicionalmente hace frente a las principales preocupaciones de los riesgos de pérdida de datos.

A través de la autenticación y la autorización, sólo aprobado y usuarios válidos pueden acceso a datos sensibles de la empresa. Con políticas establecidas y basadas en patrones se puede crear un contenedor seguro para controlar los flujos de datos, de igual manera se puede restringir el uso compartido por los usuarios, envío de archivos adjuntos y monitoreo de las acciones que se puedan efectuar como son las acciones de copiar y pegar, facilitando los controles de fuga de la información.

Los dispositivos que están perdidos, robados o comprometidos pueden ser eliminados de forma selectiva para mitigar el contenedor seguro y otras aplicaciones empresariales, como son datos o perfiles del empleado.

La plataforma MaaS360 ofrece una completa solución para la prevención de pérdida de datos con los flujos de trabajo coherente y sin fisuras. Se utiliza un enfoque de doble personalidad o perfil, manteniendo todo lo que sus usuarios necesitan para el trabajo en un lugar seguro. Pueden gestionar todos sus correos electrónicos, contactos, calendario, aplicaciones, documentos, y la Web de un espacio de trabajo dedicado en sus dispositivos móviles, independientemente de quién sea su propietario. Se puede implementar controles para gestionar el contenedor seguro que no afectan al resto del dispositivo para que pueda separar las actividades de trabajo con las actividades comunes que el empleado realiza en sus dispositivos personales.

La interoperabilidad de la solución permite incrementar la productividad de los empleados mediante el uso de herramientas de colaboración que están disponibles tanto para iOs como Android, todas necesario para garantizar un entorno seguro y protegido en cualquier momento, facilitando acceder al espacio de trabajo desde cualquier lugar, en especial desde los dispositivos de propiedad de los empleados. Todo el entorno está diseñado para trabajar con fluidez, velocidad y seguridad proporcionando una experiencia simple e intuitiva para el usuario. Entre las funcionalidades más notables de la plataforma se destaca:

- *MaaS360 Correo Seguro:* es una aplicación para la gestión de las credenciales y de información personal para el correo electrónico, calendario y contactos; permitiendo el control del correo electrónico mediante contenedores en conformidad con FIPS 140-2 y encriptando la información

mediante AES-256[23]. Tiene la compatibilidad y soporte para servicios de correo en la nube como son Office 365 y Gmail.

- *MaaS360 Aplicación de Seguridad Móvil:* permite habilitar la autenticación requerida por los usuarios para hacer cumplir los controles de conformidad y políticas de seguridad en los dispositivos. Restringe las acciones de copiar y pegar, así como las copias de seguridad de datos locales y en la nube. Adicionalmente permite recibir alertas en tiempo real de violaciones de cumplimiento y configurando las acciones a eventos y aplicaciones de manera automática. Está disponible como una aplicación que también puede integrarse con el resto de aplicaciones preexistentes en la empresa mediante el uso del SDK para la integración. Las aplicaciones tienen la funcionalidad de túnel a nivel App (sin VPN) para el acceso seguro a los datos corporativos.
- *MaaS360 Documentos compartidos seguros:* permite ver y guardar el contenido de documentos de forma segura mediante el uso de un contenedor cifrado, restringiendo el contenido que se comparte y las funciones de copiar y pegar fuera del contenedor. Es compatible con servicios de recursos compartidos como son SharePoint, Windows File Share con lo cual se añade las funciones de sincronizar o eliminar archivos. Trabaja con todos los tipos de archivos más comunes como word, excel, power point, formato de texto y pdf.
- *MaaS360 Navegador Web Seguro:* permite tener un acceso seguro a los sitios web corporativos sin la necesidad de una VPN garantizando la movilidad en sharepoint, blogs internos y sistemas ERP[24]. La seguridad URL está definida por más de 60 categorías con las cuales se puede bloquear, permitir o rastrear el acceso; así como restringir el uso de cookies, descarga de archivos e impresión desde sitios que han sido reportados mediante el sistema de alarmas de texto o HTML al administrador y usuario.

[23] (Wikipedia, 2009)**AES:** es un esquema de cifrado por bloques adoptado como un estándar de cifrado que utiliza un algoritmo de cifrado capaz de proteger la información sensible cuyas claves pueden ser de 128, 192 y 256 bits y como es el caso AES-256 utiliza claves de 256 bits.

[24] (Wikipedia, 2014) **ERP:** son sistemas de información gerenciales que integran y manejan muchos de los negocios asociados con las operaciones de producción y de los aspectos de distribución de una compañía en la producción de bienes o servicios.

El servicio de control que provee MaaS360 permite generar informes de cumplimiento en los cuales se muestran información de cumplimiento de las políticas corporativas, qué eventos ocasionan el incumplimiento (como gestor de aplicaciones de seguridad permite deshabilitarlas), y qué acciones de remediación se deben tomar en cuenta. Los informes que demuestran que los sistemas cumplan pueden ser usados para realizar auditorías de cumplimiento de regulaciones SOX, PCI, DSS, HIPAA, entre otras.

A diferencia de otras soluciones MaaS360 es una solución modular que se ofrece por paquetes o de forma individual cada módulo que puede irse acoplando con las demás soluciones dando escalabilidad e integración a los distintos ambientes empresariales.

Figura 10. Arquitectura de MaaS360: Soporte a gran volumen de dispositivos. *(MaaS360, 2015)*

Tabla 7.

MaaS360: Paquetes de distribución frente a BYOD

MÓDULOS	MAAS360 SUITES			
	Gestión Móvil Avanzada	Suite de Productividad	Compartición Segura de Documentos	Portal Empresarial Móvil
Gestión de dispositivos móviles.	✓			
Gestión de aplicaciones móviles.	✓			
Administración de gastos móviles.	✓			
MaaS360 correo seguro.		✓		
MaaS360 navegador web seguro		✓		
MaaS360 Aplicación móvil de seguridad.		✓		
Administrador móvil de contenidos.			✓	
Editor de documentos seguro.			✓	
Sincronización de documentos.			✓	
Puerto de enlace empresarial móvil para navegadores web.				✓
Puerto de enlace empresarial móvil para documentos.				✓
Puerto de enlace empresarial móvil para aplicaciones.				✓

Recuperado de: *(MaaS360, 2015)*

2.4.3. Vmware AirWatch.

Es una plataforma de gestión de movilidad empresarial en donde la transición de las herramientas estáticas están cambiando por herramientas multiplataforma y dinámicas que permiten gestionar miles de dispositivos, aplicaciones y contenidos sin la necesidad de administrar varios proveedores; estandarizando soluciones y simplificando los servicios de migración consolidando múltiples soluciones específicas en una única plataforma.

La consola de administración da visibilidad en todos los dispositivos registrados ya sean de propiedad de la empresa o propiedad de los empleados, independientemente del tipo de plataforma o dispositivo. La creación de grupos de organización proporciona a los administradores una manera ágil para gestionar todos los usuarios y dispositivos. La integración con los servicios de directorio (AD / LDAP) permite la creación de grupos basados en roles personalizados que imitan la estructura corporativa existente. La consola basada en web HTML5 se integra con los sistemas empresariales existentes y se puede acceder en cualquier momento y en cualquier lugar.

EL proceso de registro de los dispositivos proporciona un flujo de inscripción basado en un agente consistente para todas las plataformas, y permite tanto a los administradores como usuarios finales realizar el registro de los dispositivos. Cuando los usuarios se inscriben, se autentican y las restricciones apropiadas, aplicaciones y contenidos se insertan automáticamente en cada perfila asignado. Los perfiles permiten definir los ajustes empresariales, políticas y restricciones para los dispositivos sin requerir la interacción del usuario. Se puede asignar perfiles basados en el sistema operativo o el tipo de propiedad dispositivo, y desplegar a un grupo de organización, usuario o grupo de usuarios individuales. Los perfiles se pueden desplegar de forma automática a los dispositivos sobre la inscripción, y los administradores pueden empujar perfiles bajo demanda a través de redes de telecomunicaciones más comunes. Los perfiles disponibles incluyen códigos de acceso, restricciones, Wi-Fi, VPN, correo electrónico, aplicaciones, entre otros.

La seguridad para dispositivos móviles, aplicaciones y contenido es una preocupación primordial en una estrategia de gestión de la movilidad e integración con políticas de BYOD. El uso de un dispositivo de propiedad de la empresa o propiedad de los empleados, para acceder a los datos corporativos, correo electrónico y más desde sus dispositivos móviles necesita de acciones por parte de los administradores de TI las cuales requieren implementar una estrategia móvil con las políticas de seguridad fuertes.

Algunos de los beneficios de la plataforma de Vmware Airwatch para la gestión de dispositivos móviles:

- Administrar una gran cantidad y diversa de dispositivos desde una sola consola.
- Permitir que los empleados registren fácilmente sus dispositivos.
- Habilitar el acceso seguro a los recursos corporativos.
- Se integra con la infraestructura existente de la empresa.
- Soporte a los dispositivos de usuarios de propiedad corporativa y compartida.
- Ganar visibilidad en toda la implementación de dispositivos móviles.

La gestión de dispositivos es más fácil, los administradores pueden eliminar el acceso a correo electrónico corporativo, Wi-Fi y VPN cuando un empleado elimine el registro o deje la compañía. Adicionalmente permite eliminar aplicaciones internas y contenidos corporativos desde dispositivos al finalizar el ciclo de vida de los activos de la empresa.

Las funcionalidades más relevantes que presta la herramienta para la seguridad y gestión de dispositivos a través de la infraestructura empresarial son:

- *Consola de gestión individual:* la consola de administración está basada en web HTML5 que ofrece una visibilidad de todos los dispositivos registrados sean de propiedad de la empresa, de los empleados o en préstamo.
- *Arquitectura global:* grupos de organización proporcionan una manera ágil de gestionar a todos los usuarios y dispositivos. La integración con servicios de directorio (AD /LDAP) permite importar la actual estructura de servicios existente a la nueva plataforma de gestión del negocio; sincronizando múltiples dominios dentro de un solo grupo de organización y cada grupo puede tener diferentes perfiles de dispositivos, aplicaciones y contenido.
- *Registro e inscripción de dispositivos fácil:* el proceso de registro proporciona un flujo simple y robusto para todas las plataformas, permite a los administradores y usuarios finales inscribir sus dispositivos a través de varias herramientas: Agentes, código QR, correo electrónico o SMS. Autenticar los usuarios mediante varias políticas basadas en usuario / contraseña, credenciales de servicio de directorio, SAML, autenticación por token o proxy.
- *Cumplimiento automatizado:* la herramienta monitorea continuamente y a tiempo real en busca de usuarios no autorizados, dispositivos comprometidos y otros riesgos. Los administradores pueden realizar un seguimiento del cumplimiento si una amenaza es identificada, los administradores de TI están alertados al correo electrónico empresarial, las aplicaciones y los recursos pueden ser bloqueados automáticamente basado en la progresividad y acciones predefinidas.
- *Tableros de información a tiempo real:* proporcionan a los administradores una vista rápida de datos de despliegue en tiempo real de la consola de administración. Desde los cuadros de información se puede ver una representación gráfica de alto nivel de la implementación, una lista completa de dispositivos registrados y profundizar en los dispositivos de usuario y detalles específicos. Todo desde un portal personalizable, centralizado con acceso rápido a la información crítica y detallada, incluyendo el cumplimiento, aplicaciones, correo electrónico y más.

- *Comandos remotos y mensajería:* permite enviar comandos bajo demanda a los dispositivos para solicitar información y realizar acciones. Los comandos incluyen consulta dispositivo, purgar código de acceso, enviar mensaje, bloqueo de dispositivo, habilitar la interconexión de datos, vista remota, sincronización y realice un borrado a nivel empresarial o general.

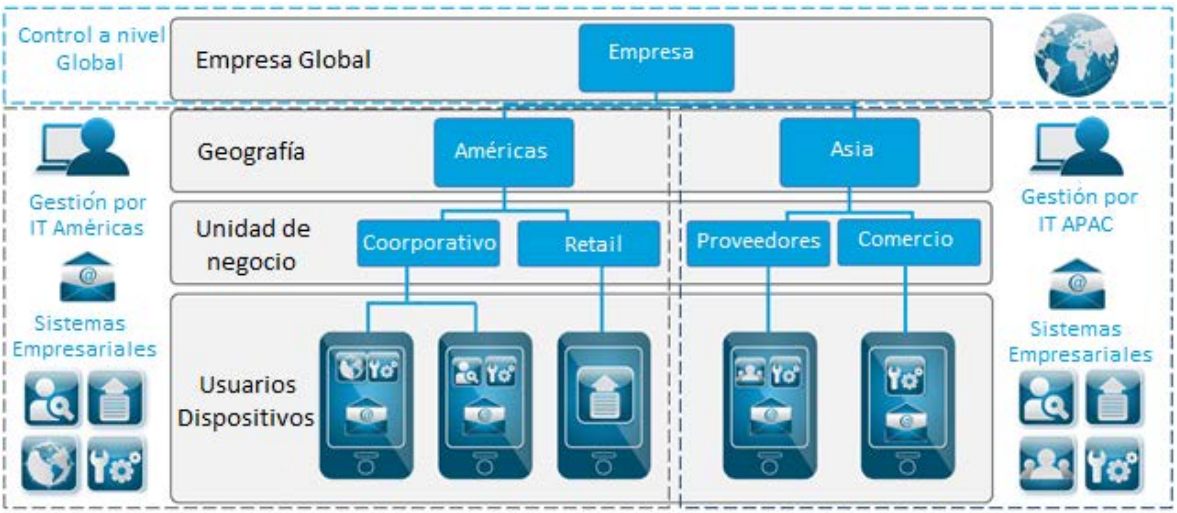

Figura 11. Arquitectura AirWatch: Integración a nivel Global *(Vmware Airwatch, 2015)*

AirWatch brinda opciones de implementación tanto en la nube como en sitio para la plataforma de administración de movilidad empresarial (EMM); permitiendo las mismas soluciones e infinitas funcionalidades de escalabilidad ofertadas tanto en la nube de AirWatch o en implementaciones en nube privada de su empresa. Si las necesidades cambian en el tiempo, se tiene la flexibilidad de migrar de un tipo de implementación a otro.

Tabla 8.

Funciones contenidas en cada suite de AirWatch

FUNCIONES	SUITES DE ADMINISTRACIÓN			
	Verde	Naranja	Azul	Amarilla
Gestión de dispositivos móviles.	✓	✓	✓	✓
Contenedor seguro.	✓	✓	✓	✓
Catálogo de aplicaciones.	✓	✓	✓	✓
Correo seguro.		✓	✓	✓
Contenedor de aplicaciones.			✓	✓
Navegador seguro.			✓	✓
Bloqueo de contenidos.			✓	✓
Bloqueo de contenidos de colaboración.				✓
Telecomunicaciones.				✓
Chat.	Complemento disponible para cualquier suite.			
Video.	Complemento disponible para cualquier suite.			

Recuperado de: *(Vmware Airwatch, 2015)*

2.5. HERRAMIENTAS LICENCIADAS.

Es el conjunto de software que son adquiridos de forma comercial con el permiso de funcionamiento, alquiler y utilización establecidos por el fabricante o desarrollador para satisfacer las necesidades del usuario o empresa que requiere las soluciones informáticas.

"Las características del software licenciado giran en torno a su comercialización y a los parámetros de distribución que establezca el productor, de acuerdo a la licenciatura respaldada por las leyes de derecho y propiedad que lo cobijen." (Oviedo, 2013)

Algunas de las características más importantes del software licenciado:

- Comercializado con ciertos términos de uso y valor.
- Establece la utilización en un número determinado de equipos.
- Se establecen relaciones comerciales, de soporte, de asesoría y capacitación entre los usuarios y asesores encargados de la distribución del producto.
- Respaldado por las leyes estatales de derecho de cada país.

La utilización de las herramientas de seguridad de la información depende del cliente, de su rol y de sus intereses de uso todo esto se tiene presente al realizar el levantamiento de los requerimientos y el caso de estudio del ambiente donde se necesitan implementar.

2.5.1. Symantec SMM.

"Symantec cuenta con el más amplio conjunto de tecnologías en una única solución para habilitar al personal móvil de manera segura. Symantec admite la administración en el nivel del dispositivo, la aplicación o los datos para resolver problemas de protección de datos y, a su vez, mejorar la experiencia de los usuarios." (Symantec, 2015)

Las herramientas de Symantec Mobility Suite permite crear controles integrales para diversos entornos móviles de cualquier dispositivo, en cualquier momento y en cualquier lugar ofreciendo productividad para las empresas y los empleados; garantizando la protección de los datos corporativos en los dispositivos, que separa la información personal y corporativa, la gestión de diversos sistemas operativos, y la prevención de los dispositivos y aplicaciones mitigando la fuga de información y evitando que el ingreso de estos nuevos dispositivos se conviertan en otro vector de ataque para la empresa.

La plataforma permite implementar una solución unificada de control que exige la seguridad consistente basada en normas de seguridad, independientemente del tipo de dispositivo, sin obstaculizar la productividad del usuario final o la intimidad personal.

De igual manera simplifica la gestión de la movilidad, la integración de la gestión de dispositivos móviles (MDM), la administración de aplicaciones móviles (MAM), la gestión de contenidos para móviles (MCM) y la protección contra amenazas móviles en una amplia consola, todo en un solo entorno ya sea estandarizado por los dispositivos de propiedad de la empresa como el ingreso de dispositivos personales de los empleados.

Algunas ventajas al usar Symantec son:

- *Gestión móvil integrada:* A través de una consola, las empresas pueden gestionar dispositivos, gestionar las aplicaciones y contenidos, datos seguros, y aplicar la protección contra amenazas en un amplio conjunto de dispositivos (iOS, Android, Windows Phone).
- *Una solución para diversos ambientes:* Si las empresas hacen cumplir un estándar a través de dispositivos de propiedad de la empresa, o desean implementar BYOD y / o políticas CYOD, TI puede aplicar un nivel constante de seguridad ofreciendo la posibilidad de crecer con las necesidades cambiantes de los teléfonos de la empresa.

- *La productividad móvil sin compromiso:* al suministrar, herramientas integrales y flexibles para asegurar los datos, aplicaciones y contenido, y gestionar la seguridad contra las amenazas, se brinda a los usuarios lo que necesitan para ser productivos sin comprometer la seguridad o la experiencia del usuario. En lugar de servir como guardianes, la empresa se convierte en un verdadero facilitador e implementador de una empresa móvil.

La plataforma de Symantec aborda todos los aspectos críticos de la movilidad empresarial incluyendo:

- *Gestión de dispositivos:* incluye, capacidades integrales de MDM escalables, proporcionando visibilidad y control sobre iOS, Android y Windows® Phone smartphones y tabletas. Los usuarios pueden inscribir fácilmente los dispositivos en su entorno empresarial, configurar y actualizar la configuración del dispositivo over-the-air[25], y proteger los dispositivos móviles con seguridad basada en certificados. Puede evitar que los dispositivos no compatibles (aparatos o dispositivos que faltan aplicaciones requeridas como jailbreak / root) se conecten a los activos empresariales, ayudando a asegurar el cumplimiento de los requisitos internos y externos de seguridad.
- *Gestión de Aplicaciones:* las aplicaciones y datos corporativos están protegidos mediante una tecnología única que envuelve en una capa de gestión y de políticas de seguridad alrededor de las aplicaciones móviles, evitando los cambios de código fuente o incrustación SDK. Esta tecnología proporciona un control granular de aplicaciones y datos corporativos con políticas dinámicas por aplicación de la conectividad, la autenticación, encriptación, acceso a datos, y el intercambio de archivos.
- *Tienda de aplicaciones empresarial:* con la colaboración de Symantec Work Hub se logra ofrecer una tienda personalizable de aplicaciones empresariales o de terceros para distribuir fácilmente entre los empleados y otros usuarios autorizados, como contratistas o socios. Los usuarios pueden ver sólo las aplicaciones que están autorizados a utilizar sobre la base de sus funciones.

[25] (Wikipedia, 2015) **Over-the-air:** se refiere a varios métodos de distribución inalámbrica de nuevas actualizaciones de software, la configuración, y la actualización de claves de cifrado a dispositivos como teléfonos móviles

Los empleados, contratistas y socios pueden estar seguros acerca de qué aplicaciones están aprobados para usar en las empresas. Los usuarios pueden calificar y comentar sobre las aplicaciones, mientras que los administradores pueden obtener informes sobre descargas de aplicaciones.

- *Aplicaciones de productividad seguros:* la plataforma incluye aplicaciones de ayuda a la fuerza laboral, lo que le permite proporcionar herramientas de productividad en un espacio de trabajo móvil seguro. Symantec Mail, una aplicación de correo electrónico basado en Microsoft Exchange ActiveSync, permite la sincronización y almacenamiento seguro del correo electrónico corporativo, calendario, contactos y más. La navegación web está protegida mediante el uso del navegador Work Web y finalmente Symantec Work File, es una aplicación de edición de archivos garantizando la gestión segura de contenidos, permite la colaboración y el acceso a los archivos corporativos. Estas aplicaciones de productividad se pueden administrar desde una consola centralizada y son instaladas a los dispositivos a través del cliente de Symantec Work Hub.
- *Programa Symantec Sealed:* permite a las empresas adoptar con confianza aplicaciones móviles de terceros mientras que satisfacen los requisitos de la seguridad de los datos. Las aplicaciones disponibles se han envuelto con una capa de seguridad y de gestión, permitiendo a TI definir políticas granulares, como la encriptación, autenticación y restricciones de intercambio de datos. Ofrece un ecosistema de confianza para asegurar las aplicaciones móviles de terceros, lo que le permite proporcionar un espacio de trabajo móvil protegido satisfaciendo las necesidades del negocio.

En adición la plataforma proporciona una potente protección, eficaz contra las amenazas maliciosas y el acceso no autorizado a la información corporativa y sensible. Aprovechando la tecnología de vanguardia, la investigación y la inteligencia de Norton Mobile Insight y Symantec Security (STAR) protegiendo los dispositivos android de riesgos de privacidad, malware y sitios fraudulentos mientras ayuda al rendimiento del dispositivo.

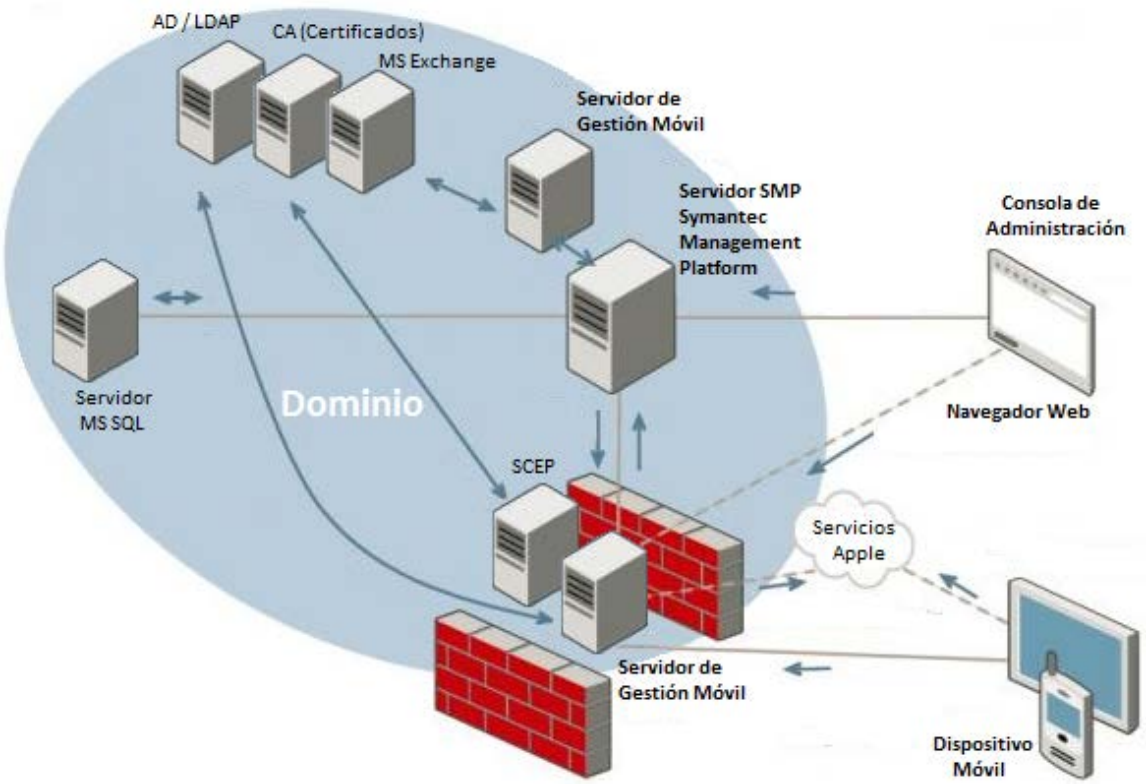

Figura 12. Symantec Mobile Management: Arquitectura Extendida a un dominio sencillo. *(Symantec, 2014)*

Las soluciones de Symantec Mobile Suite se compone por un conjunto de módulos que se acoplan y van agregando caracterizas para cada ambiente o dimensionamiento que la empresa necesite, de igual manera su solución está disponible como un servicio (SaaS) para empresas que posean la infraestructura adecuada para la solución.

Tabla 9.

Symantec SMM: Módulos y funciones

FUNCIONES	TRIAL	SUITE	GESTIÓN DE APLICACIONES	GESTIÓN DE DISPOSITIVOS	PROTECCIÓN CONTRA AMENAZAS
Tienda de aplicaciones.	✓	✓	✓	✓	
Política de aplicaciones.	✓	✓	✓		
Tienda de contenidos.	✓	✓	✓	✓	
Política de contenidos.	✓	✓	✓		
Política de dispositivos.	✓	✓		✓	
Correo seguro.	✓	✓	✓		
Navegador web seguro.	✓	✓	✓		
Editor seguro.	✓	✓	✓		
Proxy de correo seguro.	✓	✓	✓	✓	
Proxy de aplicaciones.	✓	✓	✓		
Protección contra amenazas.	✓	✓			✓
Agente móvil.	✓	✓	✓	✓	✓
Tableros de información y reportes.	✓	✓	✓	✓	✓

Recuperado de: *(Symantec, 2015)*

2.5.2. Trend Micro Mobile Security.

"Es una plataforma que permite controlar la estructura de trabajo BYOD (uso de los dispositivos propios de los empleados) gracias a la integración de características de gestión de dispositivos móviles (MDM), seguridad de dispositivos móviles, protección de datos y gestión de aplicaciones. Todo ello mediante una única solución fácil de gestionar. La integración con la consola de Trend Micro Control Manager permite centralizar las políticas y la gestión de la seguridad para puestos de trabajo de Trend Micro OfficeScan y otras soluciones de Trend Micro para aplicar una estrategia de seguridad holística." (Trend Micro, 2015)

Permite a los usuarios optimizar de forma segura la tecnología móvil en sus áreas de trabajo ayudando a encontrar el equilibrio entre el empoderamiento en los dispositivos móviles de los empleados y guiándoles a ser más productivos, brindándoles la protección de su información confidencial. Algunas de las bondades que presenta la herramienta son:

- Permite asegurar, rastrear, monitorear y administrar dispositivos móviles, aplicaciones y datos.

- Ayuda en la configuración, administración y supervisión de las amenazas y la protección de datos a través de una única consola.
- Se ejecuta como una solución independiente o se integra con otros productos de Trend Micro a través de Trend Micro Control Manager. Acorde con el fabricante para tener una solución de protección de la información de extremo a extremo sugiere la integración con Tren Micro OfficeScan.
- Reduce los costos de TI y la complejidad al habilitar los puntos finales unificados mediante una plataforma de seguridad móvil.
- Asegura la amplia gama de plataformas móviles: iOS, Android, Blackberry y Windows Phone.

Con la explosión de los dispositivos móviles en el lugar de trabajo, los empleados han reconocido lo necesidad del apoyo que se necesita para una creciente lista de nuevas formas de aprovechar esta tecnología para su trabajo.

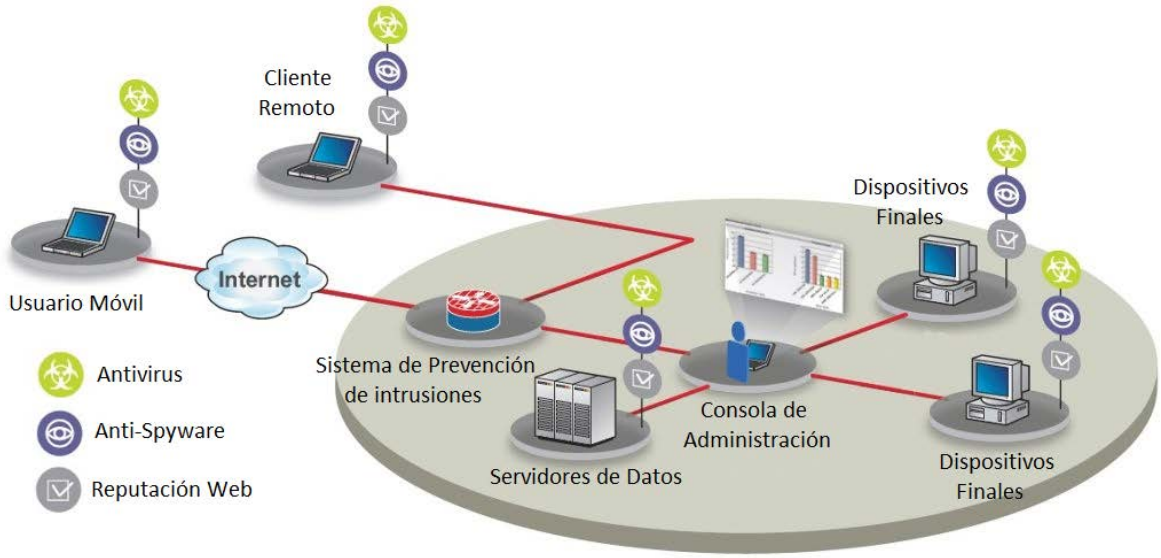

Figura 13. Trend Micro: Seguridad profunda con la integración de OfficeScan *(Haletky, 2013)*

Trend Micro Mobile Security es un componente más de la solución de protección que proporciona visibilidad y control de los dispositivos móviles, aplicaciones, y datos a través de una única consola integrada logrando el equilibrio correcto entre la productividad del usuario y los riesgos de TI. Mobile Security incluye:

- Gestión de dispositivos móviles (MDM).
- Gestión de aplicaciones móviles.

- Servicio de reputación de aplicaciones.
- Antivirus para dispositivos móviles (Android).

En los esquemas BYOD, la protección de sus puntos finales contra la evolución constante de las amenazas se ha convertido en un proceso costoso para los administradores de TI. Con dispositivos móviles y computación en la nube, la protección de los datos contra pérdida o robo es la mayor preocupación de las gerencias de TI; incrementando los problemas de rendimiento asociados con tratar de aplicar la seguridad tradicional para infraestructuras de escritorios virtuales, demostrando que es necesario una plataforma de seguridad de dispositivos finales flexible que se adapte a las necesidades cambiantes con una arquitectura orientada a mejorar el rendimiento. Las características más importantes que Trend Micro ofrece es:

- *Gestión centralizada:* simplifica la administración proporcionando un solo panel de control y un centro de gestión contra amenazas y gestión de políticas de pérdida de la información a través de las capas de la infraestructura de TI. Dando una visión única de los usuarios de la empresa desde el escritorio al dispositivo móvil con vistas de las amenazas a tiempo real ayudando a identificar amenazas avanzadas que pueden apuntar a usuarios con acceso a información crítica de la empresa, logrando la aplicación de políticas más coherentes con un solo clic en el despliegue de la protección de datos y directrices a través de dispositivo final, mensajería y soluciones de pasarela de datos ofreciendo una visibilidad sobre el número, tipo y configuración de los dispositivos.
- *Administración de aplicaciones móviles:* evita el uso no autorizado de aplicaciones riesgosas en los dispositivos conectados a la red mediante el uso de listas negras y listas blancas de aplicaciones. Ayuda a la gestión de inventario y la presentación de informes para mejorar la visibilidad de las aplicaciones usadas a través de todos los dispositivos, grupos y la empresa permitiendo incluso gestionar un bloque específico de aplicaciones basadas en categorías y desplegándolas en los dispositivos de usuario final utilizando la funcionalidad tienda de aplicaciones corporativa, facilitando el uso de las aplicaciones mediante el servicio de reputación de aplicaciones.

- *Gestión de dispositivos móviles:* permite registrar y provisionar de forma remota, dispositivos en la red corporativa ajustes tales como VPN, Exchange ActiveSync y conectividad inalámbrica. Facilita el despliegue de Apple TV y Servicios AirPrint para los usuarios de iOS. Proporciona la localización del dispositivo y registro en el inventario para asegurar el rastreo de los dispositivos tanto de propiedad de la empresa como de los empleados, ya sea que se hayan registrado o no. Integra políticas cruzadas entre dispositivos y grupos para la implementación coherente de seguridad y gestión de dispositivos autorizados mediante el uso de reglas basadas en federación de identidades mediante el uso de IMEI, Wi-Fi,y la dirección MAC.
- *Protección de Datos:* protege los datos corporativos con funciones de bloqueo remoto, geo localización del dispositivo y borrado completo o selectivo en el caso que el dispositivo móvil sea robado o perdido. La plataforma hace cumplir las normativas de seguridad y cifrado de datos facultando el bloqueo de funciones específicas de los dispositivos como son: cámara, bluetooth, conectividad 3G / 4G y lectores de tarjetas SD; otorgando una visión completa de los dispositivos que no están registrados y que aun acceden a la red corporativa, permitiendo así la implementación y configuración de contenedores para administrar los dispositivos.

Tabla 10.

Funciones disponibles en cada suite de Trend Micro Security

FUNCIONES	SUITES DE SEGURIDAD		
	Empresarial y Datos	Protección de Datos	Seguridad Empresarial
Protección en dispositivos finales y Anti-Malware.	✓		✓
Integración con escritorios virtuales (VDI[26]).	✓		✓
Servidor Anti-Malware.	✓		✓
Seguridad de Correo y Anti spam.	✓		✓
Seguridad Web y mensajería segura.	✓		✓
Control de dispositivos.	✓	✓	
DLP Integrado.	✓	✓	
MDM.	✓	✓	
Encriptación de dispositivos finales.	✓	✓	
Administración centralizada.	✓	✓	✓

Recuperado de: *(Trend Micro, 2015)*

2.5.3. IBM Security Endpoint Manager.

IBM Endpoint Manager utiliza la tecnología BigFix[27] potenciándola como una herramienta de administración remota utilizada para prestar servicios de apoyo en los dispositivos finales administrados ya sean estos ordenadores Windows y Mac de escritorio o móviles que reciben soporte estándar.

Es una completa plataforma de productos, basados en tecnología BigFix, que ayudan a conseguir una seguridad y gestión de puntos finales más rápida e inteligente. Estos productos le permiten ver y gestionar puntos finales físicos y virtuales, incluidos servidores, sistemas de escritorio, portátiles, smartphones, tabletas y equipos especializados como dispositivos de punto de venta, cajeros y quioscos de autoservicio. Permitiendo remediar, proteger y crear informes prácticamente en tiempo real. IBM Security Endpoint Manager

[26] (Wikipedia, 2015). **VDI:** comúnmente conocido como "Virtual Desktop infraestructura" es el conjunto de varias instancias de sistemas operativos de escritorio en una plataforma de hardware de servidor que ejecuta un hipervisor.

[27] (IBM, 2015) **BigFix:** era una compañía americana centrada en reducir el costo y la complejidad de la administración de equipos de escritorio, móviles y de servidores en red. Inició como aplicación de soporte para PC, que luego se expandieron para permitir la entrega de una amplia variedad de servicios de gestión de punto final incluyendo inventario de activos / descubrimiento, detección de vulnerabilidades de seguridad y la remediación, la distribución de software, informes de cumplimiento, parches de gestión, administración de licencias de software, aplicación de políticas de seguridad y gestión del consumo de energía del dispositivo de punto final. Posteriormente BigFix fue comprada por IBM e integrada a sus soluciones empresariales.

permite cubrir las necesidades desde medianas y grandes empresas mediante su solución modular y escalable brindando ediciones acordes a la necesidad que se desea cubrir:

IBM Endpoint Manager for Core Protection: ofrece una protección a tiempo real en los dispositivos finales físicos y virtuales frente a malware y otras amenazas que se pueden encontrar por la red a través de un sistema de reputación web y de archivos, contiene un poderoso cortafuego y la integración de análisis de comportamiento de los procesos y tareas en los dispositivos finales.

IBM Endpoint Manager for Datacenters: permite a los administradores de TI realizar las tareas de automatización entre servidores, otorgando la facilidad en la detección de problemas en los dispositivos finales independientemente del sistema operativo que estos tengan y el tipo de conexión que mantengan con el servidor. Adicionalmente proporciona scripts o plantillas prediseñadas que ayudan a la creación de flujos de automatización suministrando escalabilidad en las aplicaciones empresariales.

IBM Endpoint Manager for Mobile Devices: permite gestionar los dispositivos móviles mayormente conocidos como son Apple iOS, Google Android, Nokia Symbian y Micrpost Windows permitiendo administrar los problemas de seguridad y complejidad dando una guía base para la implementación de las políticas BYOD y cumplimiento de normativas de seguridad de la información.

IBM Endpoint Manager for Lifecycle Manager: ayuda a la gestión de las tareas operativas del área de TI entre sus principales funciones se tiene:

- Descubrimiento de todos los dispositivos habilitados para conexión de red.
- Inventario de dispositivos mediante el escaneo profundo y listado de sus atributos de hardware y software.
- Gestión y control remoto mediante Windows Remote Desktop y la funcionalidad de asistencia y sesiones remotas mediante Tivoli[28].
- Automatización en la distribución de software añadiendo niveles de control en el proceso de implementación de software.
- Despliegue de sistemas operativos proporciona la creación de imágenes completas y aprovisionamiento de sistemas operativos.

[28] (IBM, 2014) **Tivoli:** es actualmente conocida como una familia de software de IBM para la administración de infraestructura de tecnología de la información.

- Análisis de uso del software ofrece el descubrimiento y análisis de aplicaciones de software instaladas en el entorno de trabajo.

IBM Endpoint Manager for Security and Compliance: es la plataforma de solución única para la gestión de seguridad de todos los dispositivos distribuidos en los entornos de red proporcionando directrices para los estándares de gobierno e industria mediante la gestión de vulnerabilidades y remediaciones de las alertas de seguridad acorde a la conformidad de varios institutos de seguridad entre ellos SANS[29]. Permite la gestión centralizada de dispositivos de múltiples proveedores de antimalware y firewall.

IBM Endpoint Manager for Patch Management: es la solución única para gestionar el despliegue de parches para Windows, Linux, UNIX y Mac en los dispositivos finales. Se encuentra monitoreando continuamente el entorno para aplicar automáticamente los parches necesarios, reduciendo los tiempos de actualización de semanas y días a horas y minutos asegurando informes sobre la implementación de parches en tiempo real.

IBM Endpoint Manager for Power Management: permite la aplicación de las políticas de conservación de energía en toda la organización y proporciona informes detallados que dan visibilidad en el uso de energía permitiendo proyectar ahorros potenciales usando un simulador del escenario para identificar problemas de configuración y automáticamente remediarlos.

El uso de IBM Endpoint Manager permite gestionar la infraestructura de TI de forma escalable basado en la arquitectura cliente servidor de N capas, permitiendo administrar computadores de escritorio, portátiles, servidores y dispositivos móviles que utilizan la infraestructura de red existente, reforzando el cumplimiento de políticas de seguridad mediante la detección automática de nuevos dispositivos y generación de informes con las remediaciones a las posibles fallos o violaciones de seguridad con visibilidad a tiempo real.

[29] (Wikipedia, 2013) **SANS:** es una institución con ánimo de lucro fundada en 1989, con sede en Maryland, Estados Unidos; que agrupa a 165.000 profesionales de la seguridad informática cuyo principal objetivo es investigar, capcacitar y certificar a los profesionales en el ámbito de seguridad informática.

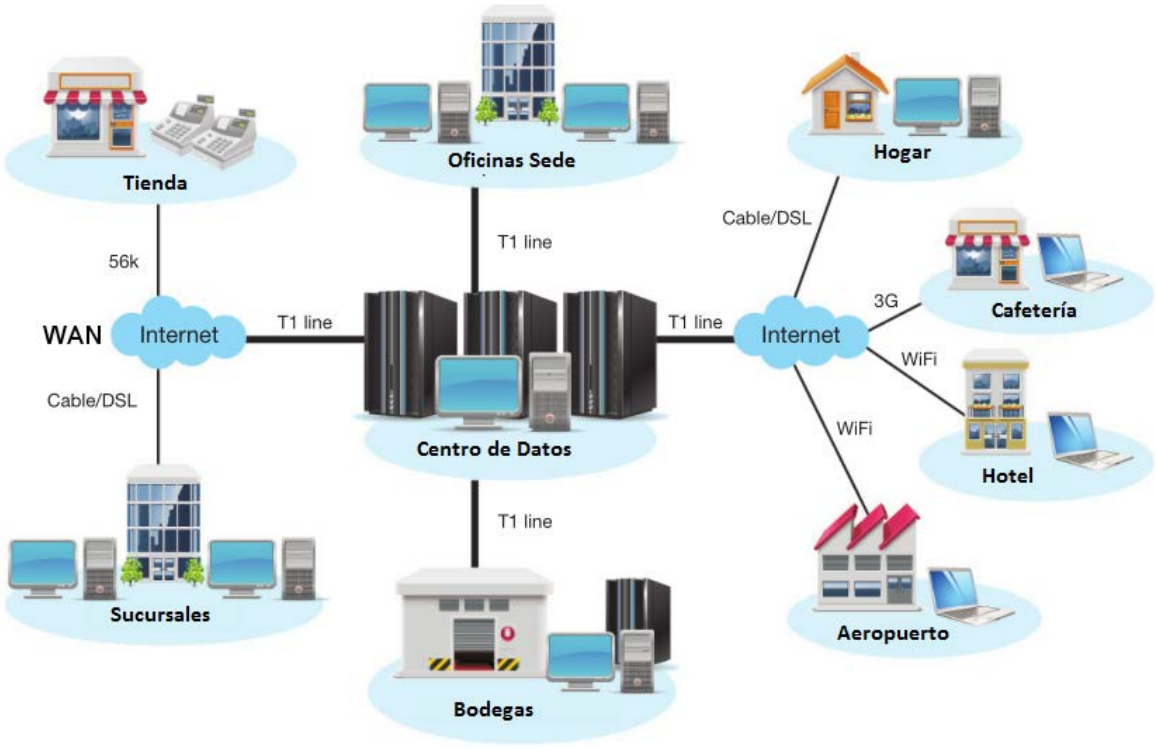

Figura 14. Interconectividad de IBM Endpoint Manager *(IBM, 2013)*

A continuación se detalla las funciones de cada módulo de la plataforma de IBM Endpoint Manager:

Lifecycle Management

- Gestión de parches.
- Inventario de SW y HW.
- Distribución de Software.
- Despliegue de S.O.
- Control Remoto.

Paquete Básico

Server Automation

- Automatización secuencial de tareas entre servidores.
- Gestión de Middleware[30].
- Despliegue de S.O. multiplataforma.
- Administración de servidores virtuales y físicos.

Core Protection

- Anti-malware.
- Firewall.
- Protección de Datos (complemento).

Software use Analysis

- Inventario de software.
- Informe de software en uso.
- Catálogo de software.

Patch Management

- Parche de S.O.
- Parche de Aplicaciones.
- Parche de máquinas virtuales.

Security & Compliance

- Gestión de parches.
- Gestión de configuración de seguridad.
- Evaluación de vulnerabilidad.
- Análisis de cumplimiento.
- Gestión de protección de dispositivos finales de terceros.
- Auto cuarentena.

Paquete Básico

Mobile Devices

- Gestión de dispositivos móviles.
- Gestión de aplicaciones.
- Contenedor de información personal en aplicaciones.
- Cumplimiento de políticas de seguridad.

Power Management

- Soporte a Windows y Macs.
- Informe de reducción de costos de recursos energéticos.
- Interfaz de información para usuario final.

[30] (Wikipedia, 2014) **Middleware:** es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos.

2.6.GESTIÓN DE DISPOSITIVOS.

Las soluciones de gestión de dispositivos finales utilizan un método proactivo y por capas para gestionar y proteger la seguridad de la empresa. Estas soluciones afrontan los riesgos de seguridad que surgen de nuevas variables y, al mismo tiempo, garantizan la disponibilidad de los dispositivos finales ya sean en sitio o móviles para maximizar la productividad de los empleados. Estas soluciones permiten que el personal de TI realice el seguimiento y supervise los dispositivos que se utilizan en toda la empresa, incluidos los que son propiedad de los empleados y los que son propiedad de la empresa.

La mayor parte de las soluciones gestiona los dispositivos de una manera similar ya que son principalmente una herramienta de administración de la configuración de políticas en los dispositivos móviles y finales, tales smartphones y tabletas. Estas herramientas ayudan a las empresas a gestionar la transición a un entorno de cómputo más complejo y de comunicaciones móviles brindando soporte a la seguridad, los servicios de red, software y administración de hardware a través de múltiples plataformas y de sistemas operativos. El principal modelo de distribución es de forma local pero también se los puede adquirir de manera de servicio (SaaS) a través de la nube. En el siguiente cuadro se puede observar las principales características de cada una de las soluciones analizadas:

Tabla 11.

Comparación de funciones de las herramientas de seguridad

LEYENDA	
✓	= disponible.
✗	= no disponible.
=	= en desarrollo.
En blanco	= indeterminado.

	CITRIX XenMobile	MaaS360 by Fiberlink	airwatch	Symantec.	TREND MICRO	
SOLUCIÓN ADMINISTRABLE.	✓	✓	✓	✓	✓	✓
DISPONIBILIDAD						
SaaS.	✓	✓	✓	✓	✗	=
Equipo (Appliance).	✓	✗	✓	✗	✗	✗
Software Windows.	✓	✓	✓		✓	✓
Software Mac.	✓	✓	✗	✗	✓	✓
Software Unix.						=
Máquina Virtual.	✗	✗	✓	✓	✗	=
Distribuidor Personalizado.	✓	✓	✓	✓	✓	✓

LICENCIAMIENTO						
Licencia Perpetua.	✓	✓	✓	✓	✓	✓
Licencia Recurrente.	✓	✓	✓	✓	✓	✓

MANTENIMIENTO						
Al comprar el producto.	✓	✓	✓	✓	✓	✓
Incluye sub-ediciones.	✓	✓	✓	✓	✓	✓
Incluye versiones superiores.	✓	✓	✓	✓	✓	✓
Soporte incluido.	✓		✓		✓	

SOPORTE						
12 x 5	✓	✓	✓	✓	✓	✓
12 x 7	✓	✓	✓	✓	✓	✓
24 x 7	✓	✓	✓	✓	✓	✓

ESCALABILIDAD Y ADMINISTRACIÓN						
Por Ubicación.	✓	✓	✓	✓	✓	✓
Ubicación Específica.	✓	✓	✓	✓	✓	✓
Administración basada en roles.	✓	✓	✓	✓	✓	✓

TOLERANCIA A FALLOS						
Soporte a servidor independiente.	✓	✓	✓	✓	✓	✓
Tolerancia a fallos.	✓	✓	✓	✓	✓	✓
Balanceo de carga.	✓	✓	✓	✓	✓	✓

ENROLAMIENTO						
Portal Web.	✓	✓	✓	✓	✓	✓
iOS App.	✓	✓	✓	✓	✓	✓
API.	✓	✓	✓	✓	✓	✓
Inscripción masiva.	✓	✓	✓	✓	✓	✓

AUTENTICACIÓN						
Directorio activo.	✓	✓	✓	✓	✓	▬
Servicio de directorios abiertos.	✓	✓	✓	✓	✓	▬
Otros LDAP.		✓	✓	✓	✓	▬
Cargas por usuario.	✓	✓	✓		✓	✓

CARACTERÍSTICAS DE CONFIGURACIÓN MÓVIL						
Requiere contraseña.	✓	✓	✓	✓	✓	✓
Restricciones en los dispositivos.	✓	✓	✓	✓	✓	✓
Cuenta Exchange de referencia.	✓	✓	✓	✓	✓	✓
Configuración WIFI.	✓	✓	✓	✓	✓	✓
VPN-L2TP.	✓	✓	✓	✓	✓	✓
VPN-Cisco AnyConnect.	✓	✓	✓	✓	✓	✓
VPN-Juniper.	✓	✓	✓	✓	✓	✓
VPN-F5.	✓	✓	✓	✓	✓	✓

CARACTERÍSTICAS iOS						
Fomentar aplicaciones menores.	✓	✓	✓	✓		✓
Correo encriptado.	✓	✓	✓	✓	✓	✓
Entorno controlado de correo Sandbox.	✓	✓	✓	✓	✓	✓
Prevención en iCloud.	✓	✓	✓	✓	✓	✓
Unión automática de WIFI.	✓	✓	✓	✓	✓	✓

CARACTERÍSTICAS BAJO DEMANDA						
Quitar contraseña.	✓	✓	✓	✓	✓	✓
Bloqueo remoto	✓	✓	✓	✓	✓	✓
Borrado remoto.	✓	✓	✓	✓	✓	✓
Envío de mensajes de texto.	✓	✓	✓	✓	✓	✓

CARACTERÍSTICAS POR PERFIL						
Inicio programado (fecha).	✓	✓	✓		✓	✓
Finalización programada (fecha).	✓	✓	✓		✓	✓
Control de versiones.	✓	✓	✓	✓	✓	✓
Regresión del dispositivo.		✓	✓			✓
Activación por inventario.		✓	✓			✓

ADMINISTRACIÓN DE APLICACIONES						
Fomentar aplicaciones web.	✓	✓	✓	✓	✓	✓
Catálogo de aplicaciones en sitio.	✓	✓	✓	✓	✓	✓
Aplicaciones menores recomendadas.	✓	✓	✓	✓	✓	✓
Integración con VPP[31].	✓	✓	✓	✓	✓	✓

CONSOLA DE ADMINISTRACIÓN						
Web.	✓	✓	✓	✓	✓	✓
API[32] o SDK[33].	✓	✓	✓	✓	✓	✓
Aplicación de escritorio.	✓	✗	✗	✓	✓	✓
Alerta cuando no hay repuesta.	✓	✓	✓	✓	✗	✓
Alerta en itinerancia (roaming).	✓	✓	✓	✓	✗	=
Alerta de aplicaciones prohibidas.	✓	✓	✓	✓	✓	✓

EXPORTACIÓN DE DATOS						
Inventario de aplicaciones.	✓	✓	✓	✓	✓	✓
Historial del dispositivo.	✓	✓	✓	✓	✓	✓
Estado del dispositivo.	✓	✓	✓	✓	✓	✓

[31] (Apple, 2015) **VPP:** son las siglas en inglés para denotar el programa de compra por volumen en el cual se acuerdan regalías por volúmenes entregados de hardware o software.

[32] (Wikipedia, 2015) **API:** es la interfaz de programación de aplicaciones, es el conjunto de subrutinas, funciones y procedimientos o métodos, que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.

[33] (Wikipedia, 2015) **SDK:** es generalmente un conjunto de herramientas de desarrollo de software que le permite al programador crear aplicaciones para un sistema en concreto.

INTEGRACIÓN						
Apple GSX.	✗	✗	✗	✗	✗	=
Microsoft BPOS		✓	✓	✓		
GOOD		✗				✗
BES		✓	✓	✗		✗

CARACTERÍSTICAS CERTIFICADAS						
SCEP Empresarial.	✓	✓	✓	✓		=
CA local con SCEP.	✓	✓	✓	✓		=
Aplica certificado para Exchange.	✓	✓	✓	✓	✓	✓
Aplica certificado para VPN.	✓	✓	✓	✓	✓	✓
Aplica certificado para WIFI.	✓	✓	✓	✓	✓	✓

LDAP						
Políticas dinámicas por grupo LDAP.	✓	✓	✓	✓	✓	=
Políticas dinámicas por LDAP OU.	✓	✓	✓	✓	✓	=
Políticas dinámicas por atributo LDAP.	✓	✓	✓	✓	✓	=
Mensajes por atributos de LDAP.	✓	✓	✓	✓	✓	=

DISPOSITIVOS SOPORTADOS						
Android.	✓	✓	✓	✓	✓	✓
Blackberry.	✓	✓	✓	=	✓	=
Symbian.	✓	✓	✓	✓	✓	✓
Windows Mobile.	✓	✓	✓	✓	✓	✓
Windows Phone 7.	✓	✓	✓	✓	✓	✓
Windows PC.		✓	✗			✓
Mac PC.		✓	✓			✓
Linux PC.		✗	✗			✓

Recuperado de: *(Vásquez Villacreses, 2015)*

IBM Endpoint Manager ha sido el líder en seguridad en dispositivos por varios años, inlcuso desde que las primeras tecnologías de administración de dispositivos fueron introducidas. IBM ha invertido continuamente en el desarrollo de nuevas tecnologías para la seguridad de la información, acoplando e integrando varias empresas que han destacado y fortalecido su amplio portafolio de soluciones como son Tivoli y BigFix; ayudando a sus clientes a hacer evolucionar hacia nuevos modelos de negocios globales, más inteligentes y centralizados.

Como se pudo observar en la tabla comparativa y en la descripción de la solución ofertada por IBM, que su solución cubre de extremo a extremo gran parte de la demanda para hacer frente las empresas a la tendencia BYOD brindando una solución robusta, escalable y granular que se puede implementar en ambientes híbridos sean estos servicios en la nube como en sitio. En consecuencia se escoge la solución de IBM para desarrollar la

presente disertación como una herramienta confiable para la seguridad de la información en dispositivos finales.

CAPÍTULO 3. IBM SECURITY ENDPOINT MANAGER

3.1. INTRODUCCIÓN.

Es una completa plataforma de productos, basados en tecnología BigFix, que ayudan a conseguir una seguridad y gestión de puntos finales más rápida e inteligente. Estos productos le permiten ver y gestionar puntos finales físicos y virtuales, incluidos servidores, sistemas de escritorio, portátiles, smartphones, tabletas y equipos especializados como dispositivos de punto de venta, cajeros y quioscos de autoservicio.

Tras analizar algunas herramientas de seguridad de la información que se hacen mención en Gartner, se hará énfasis en la plataforma de IBM ya que es en la que se tiene dispone más experiencia en implementación y despliegue para lo cual en el siguiente capítulo se creará una guía de dimensionamiento e instalación de la solución para un entorno cliente servidor, y dando un preámbulo a las funciones básicas que se disponen.

3.2.REQUERIMIENTOS Y MODELAMIENTO DEL AMBIENTE.

Los "requisitos de negocio" de la compañía debe estar direccionada para gestionar de forma centralizada los puntos finales distribuidos y proporcionar parches y capacidad de gestión de cumplimiento de políticas de seguridad. La empresa tiene que cubrir todo el conjunto de sistemas de TI, incluyendo todas las plataformas, como Microsoft Windows, Linux, AIX y Solaris UNIX. Después que todos los sistemas y dispositivos estén registrados, la empresa puede comenzar a poner en práctica las soluciones de parcheo y de cumplimiento de seguridad.

La solución de todo el sistema debe ser compatible con operaciones globales al tiempo que proporciona un control centralizado. El sistema debe cumplir tanto con la política corporativa y de política de TI local. También debe ser compatible con la futura expansión de los sitios existentes y la adición de sitios. Todas las necesidades de negocios deben cumplir con los recursos actuales o menor número del personal de TI para luego poder implementar procesos de auditoría para manejar los controles internos y de regulación de la industria, tales como Basel, Sarbanes-Oxley (SOX), y Payment Card Industry - Data Security Standard (PCI-DSS).

La primera fase del proyecto debe abordar los controles internos y los requisitos de auditoría, para mejorar la visibilidad de las empresas del entorno activo y TI. En la segunda

fase, la empresa implementa las regulaciones de la industria sobre la base de las prioridades y necesidades para integrar procesos y herramientas de TI que mejoran la capacidad de recuperación y apoyan la estrategia de expansión global.

3.2.1. Dimensionamiento de la herramienta

Durante el levantamiento de requerimientos es importante delimitar los objetivos que la empresa desea alcanzar con la implementación de las soluciones y validar las medidas de seguridad adicionales que la empresa necesita implementar, y así determinar las soluciones específicas que potencialmente pueden cumplir los requisitos funcionales. Al utilizar el Plan de Seguridad de IBM, se puede mapear los requisitos funcionales en artefactos arquitectónicos específicos, la identificación de las soluciones adecuadas para aplicar o que están acorde al modelado del ambiente de la empresa; para lograrlo es necesario conocer los componentes del framework de seguridad a detalle.

Figura 15. Framework de Seguridad IBM *(Darnalt C. , 2013)*

3.2.2. Hardware soportado

La siguiente tabla identifica los productos disponibles en la familia de productos de IBM Endpoint Manager 9.2.0, en la cual se pueden observar los requisitos del sistema en diferentes niveles y organización a detalle. La Plataforma IEM se incluye junto con todos los productos con licencia en IBM Endpoint Manager para proporcionar los detalles de

soporte completos de la infraestructura, además de las capacidades de soporte de los productos individuales.

Tabla 12.

Sistemas Soportados por IBM Endpoint Manager 9.2

IBM ENDPOINT MANAGER PLATFORM 9.2.0

SISTEMA OPERATIVO		SISTEMA MÍNIMO	HARDWARE
AIX	AIX 6.1	TL4	POWER System - Big Endian
	AIX 7.1	Sistema Base	POWER System - Big Endian
HP	HP-UX 11i v1	Sistema Base	PA-RISC
	HP-UX 11i v2	Sistema Base	PA-RISC
	HP-UX 11i v3	Sistema Base	PA-RISC
	HP-UX 11i v2	Sistema Base	iA64
	HP-UX 11i v3	Sistema Base	iA64
Linux	CentOS 5.3	Sistema Base	x86-32 / x86-64
	CentOS 6.0	Sistema Base	x86-32 / x86-64
	Debian 6.0	Sistema Base	x86-32 / x86-64
	Debian 7.0	Sistema Base	x86-32 / x86-64
	Red Hat Enterprise Linux 5 Advanced Platform	Sistema Base	x86-32 / x86-64
	Red Hat Enterprise Linux 5 Server	Sistema Base	x86-32 / x86-64
	Red Hat Enterprise Linux 6 Server	Sistema Base	x86-32 / x86-64
	Red Hat Enterprise Linux 6 Server	Sistema Base	IBM z Systems / POWER System - Big Endian
	Red Hat Enterprise Linux 7 Server	Sistema Base	x86-32 / x86-64
	SUSE Linux Enterprise Server 10	Sistema Base	x86-32 / x86-64
	SUSE Linux Enterprise Server 10	Sistema Base	IBM z Systems / POWER System - Big Endian
	SUSE Linux Enterprise Server 11	Sistema Base	x86-32 / x86-64
	SUSE Linux Enterprise Server 11	Sistema Base	IBM z Systems / POWER System - Big Endian
	SUSE Linux Enterprise Server 12	Sistema Base	x86 -64
	Ubuntu 10.04 LTS	Sistema Base	x86-32 / x86-64
	Ubuntu 12.04 LTS	Sistema Base	x86-32 / x86-64
	Ubuntu 14.04 LTS	Sistema Base	x86-64
Mac OS	OS X Snow Leopard 10.6	Sistema Base	x86-32 / x86-64
	OS X Lion 10.7	Sistema Base	x86-64
	OS X Mountain Lion 10.8	Sistema Base	x86-64
	OS X Mavericks 10.9	Sistema Base	x86-64
	OS X Yosemite 10.10	Sistema Base	x86-64
Solaris	Solaris 10	Sistema Base	SPARC
	Solaris 10	Sistema Base	x86-32 / x86-64

	Solaris 11	Sistema Base	SPARC
	Solaris 11	Sistema Base	x86-64
Windows	Windows 8.1 Enterprise	Sistema Base	x86-64
	Windows 8.1 Professional	Sistema Base	x86-32 / x86-64
	Windows 8.1 Standard	Sistema Base	x86-32 / x86-64
	Windows 8 Enterprise	Sistema Base	x86-64
	Windows 8 Professional	Sistema Base	x86-32 / x86-64
	Windows 8 Standard	Sistema Base	x86-32 / x86-64
	Windows 7 Home	Sistema Base	x86-32 / x86-64
	Windows 7 Professional	Sistema Base	x86-32 / x86-64
	Windows 7 Enterprise	Sistema Base	x86-32 / x86-64
	Windows Embedded POSReady 7	Sistema Base	x86-32
	Windows Embedded Standard 2009	Sistema Base	x86-32
	Windows Embedded POSReady 2009	Sistema Base	x86-32
	Windows Server 2003 R2 Standard Edition	SP2	x86-32 / x86-64
	Windows Server 2003 R2 Datacenter Edition	SP2	x86-32 / x86-64 / ia64
	Windows Server 2003 Enterprise Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2003 Standard Edition	SP2	x86-32 / x86-64 / ia64
	Windows Server 2008 Datacenter Edition	SP2	x86-32 / x86-64
	Windows Server 2008 R2 Datacenter Edition	Sistema Base	x86-64
	Windows Server 2008 Enterprise Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2008 R2 Enterprise Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2008 Standard Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2008 R2 Standard Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2012 Datacenter Edition	SP2	x86-32 / x86-64
	Windows Server 2012 R2 Datacenter Edition	Sistema Base	x86-64
	Windows Server 2012 Enterprise Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2012 R2 Enterprise Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2012 Standard Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Server 2012 R2 Standard Edition	Sistema Base	x86-32 / x86-64 / ia64
	Windows Vista Business	Sistema Base	x86-32 / x86-64
	Windows Vista Enterprise	Sistema Base	x86-32 / x86-64
	Windows XP Professional	SP2	x86-64

	Windows XP Professional		SP3	x86-32
Hypervisor	AIX	IBM PowerVM Hypervisor (LPAR, DPAR, Micro-Partition)		
		WPAR: Product installed in System Workload Partition AIX 6.1		
	Linux	IBM PR/SM any version.		
		IBM PowerVM Hypervisor (LPAR, DPAR, Micro-Partition		
		KVM in SUSE Linux Enterprise Server (SLES) 11		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 5.6		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 6.0		
		VMware ESX 4.0		
		VMware ESX 4.1		
		VMware ESXi 4.0		
		VMware ESXi 4.1		
		VMware ESXi 5.0		
		VMware ESXi 5.1		
		VMware ESXi 5.5		
		z/VM 6.1		
	MacOS	KVM in SUSE Linux Enterprise Server (SLES) 11		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 5.6		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 6.0		
		VMware ESX 4.0		
		VMware ESX 4.1		
		VMware ESXi 4.0		
		VMware ESXi 4.1		
		VMware ESXi 5.0		
		VMware ESXi 5.1		
		VMware ESXi 5.5		
	Solaris	KVM in SUSE Linux Enterprise Server (SLES) 11		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 5.6		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 6.0		
		VMware ESX 4.0		
		VMware ESX 4.1		
		VMware ESXi 4.0		
		VMware ESXi 4.1		
		VMware ESXi 5.0		
		VMware ESXi 5.1		
		VMware ESXi 5.5		
	Windows	KVM in SUSE Linux Enterprise Server (SLES) 11		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 5.6		
		Red Hat KVM as delivered with Red Hat Enterprise Linux 6.0		
		VMware ESX 4.0		
		VMware ESX 4.1		
		VMware ESXi 4.0		
		VMware ESXi 4.1		
		VMware ESXi 5.0		
		VMware ESXi 5.1		
		VMware ESXi 5.5		

Recuperado de: *(IBM, 2015)*

3.3. GUÍAS DE IMPLEMENTACIÓN Y DESPLIEGUE.

Antes de implementar la herramienta, se debe seleccionar el tipo de despliegue ya que se puede optar por una instalación de evaluación o de producción.

Si elige la instalación de evaluación, se podrá implementar Endpoint Manager Server para un período de 30 días para lo cual no es necesario adquirir una licencia.

Por otro lado si se contempla realizar la instalación de producción se debe adquirir una licencia. Cuando se reciba el archivo de autorización de licencia de IBM Endpoint Manager, se podrá crear un sitio de administración y gestión de instalación personalizada que, a su vez, le permite instalar y utilizar IBM Endpoint Manager.

3.3.1. Instalación

Un despliegue simplificado IBM Endpoint Manager comprende al menos un servidor que recoge Fixlets[34] de Internet donde pueden ser vistos por el operador de la consola y se distribuyen a equipos con la función de retrasmitir la información colectada a los clientes (Relay). Cada cliente inspecciona su entorno informático local y reporta cualquier Fixlets pertinentes a los Relays, que comprime los datos y pasa de nuevo a los servidores.

La consola de IBM supervisa toda esta actividad. Se conecta a los servidores y actualiza periódicamente sus pantallas para reflejar los cambios o nuevos conocimientos acerca de la red permitiendo al operador de la consola tomar acciones a los equipos apropiados para corregir las vulnerabilidades, aplicar políticas de configuración, despliegue de software, y así sucesivamente en tiempo real.

Luego de definir el tipo de implementación a efectuar y un servidor de seguridad activa en el equipo donde va a instalar el servidor, se debe configurar la instalación de las siguientes maneras:

Instalación Interactiva: durante una instalación interactiva, los programas de instalación detectan si un servidor de seguridad local está activo y se puede especificar si desea configurarlo para el servidor de punto final.

[34] (IBM, 2015) **Fixlets:** se definen como las acciones que se consideran exitosos cuando su relevancia se evalúa como falsa. Estas pueden clasificarse ya sea como una "tarea" en función de sus necesidades organizativas o como una acción en respuesta a una alerta.

Instalación Silenciosa: mediante la instalación silenciosa, puede establecer `CONF_FIREWALL = YES` en el archivo de respuestas para exigir la configuración del firewall. Para lo cual hay que especificar los dos puertos para recibir comunicación de entrada y salida:

- 52311 Puerto para UDP y TCP / IP
- 80 para Web Reports y TCP / IP

Para iniciar la instalación se debe descargar IBM Endpoint Manager desde el portal de IBM Passport Advantage o desde el portal de soporte de IBM: http://support.bigfix.com/bes/install/downloadbes.html. De igual manera si solo se va a realizar una evaluación o demostración del producto se lo puede obtener desde el portal DeveloperWorks: http://www.ibm.com/developerworks/downloads/tiv/endpoint/, ambos instaladores son los mismos para un despliegue tanto de producción como evaluación.

Para obtener el componente de servidor descarga los siguientes archivos de Passport Advantage:

Tabla 13.

Descripción del software IBM

DESCRIPCIÓN	No. DE PARTE	ARCHIVO
IBM Endpoint Manager Platform Install V9.2 for Multiplatforms	CN1QXML	IBM Endpoint Manager 9.2.0.363.zip

Recuperado de: *(IBM, 2015)*

Para extraer los archivos del servidor en Windows, realizamos los siguientes pasos:

1. Copie el archivo zip del Administrador de Endpoint IBM Endpoint Manager 9.2.0.363.zip a su Windows Server.
2. Expanda el archivo zip con el siguiente comando:

```
unzip "IBM_Endpoint_Manager 9.2.0.363.zip"
```

A continuación se puede encontrar el archivo `setup.exe` para instalar el servidor de Windows en la carpeta IBM Endpoint Manager 9.2.0.363.

3.3.2. Ingreso de licencia

Al iniciar el proceso de instalación del producto se solicitara el ingreso del archivo de licenciamiento de la consola de administración el mismo que tiene extensión

*.BESLicenseAuthorization, y que lo pueden obtener mediante el centro de claves o de tratarse de una evaluación o prueba de concepto mediante un representante o técnico preventa de IBM.

Cuando ya disponemos del archivo de autorización de licencia, se debe solicitar un certificado de licencia y luego crear una cabecera web personalizada que, a su vez, le permite instalar y utilizar IBM Endpoint Manager. La cabecera incluye direcciones URL de los programas CGI de servidor y otro sitio de información en un archivo MIME firmado. La creación de la cabecera es fundamental para el acceso y la autenticación de su sitio de acción. Para crear la cabecera y activar su sitio, se debe seguir los siguientes pasos:

1. Ejecute el Administrador de instalación de IBM Punto BigFix-BES-9.2.0.xxxx.exe, donde 9.2.0.xxxx es la versión del instalador). Cuando se solicite, se seleccionará la instalación de producción y se acepta el Acuerdo de licencia de software. En la pantalla de bienvenida, hacemos clic en Siguiente.
2. Después de leer y aceptar el contrato de licencia, se debe seleccionar Deseo instalar con un archivo de autorización de licencia de IBM Endpoint Manager, para crear la clave privada y cabecera.

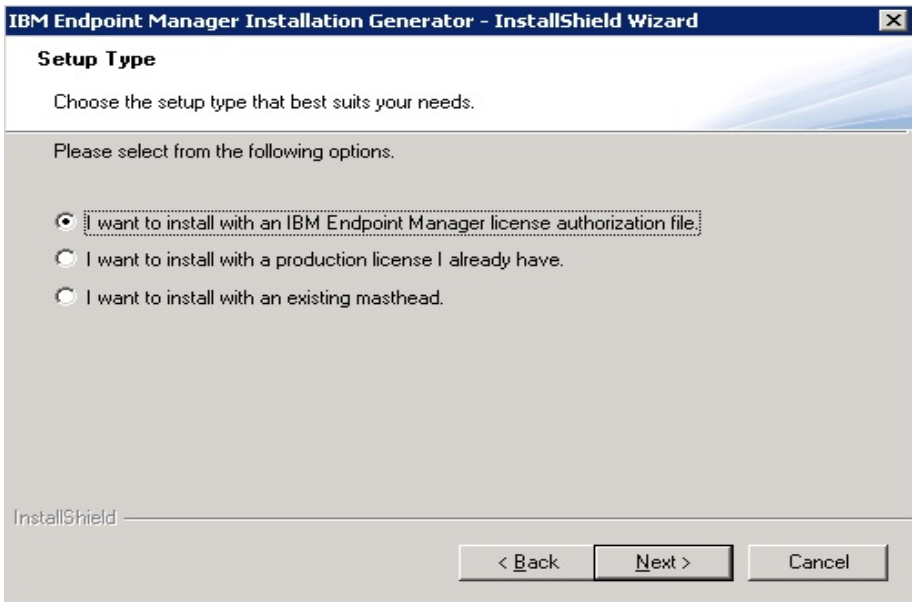

Figura 16. IBM Endpoint Manager Generador de Instalador. (Vásquez Villacreses, 2015) (IBM, 2013)

3. Se especifica la ubicación de su archivo de autorización de licencia, que tiene un nombre como `CompanyName.BESLicenseAuthorization`

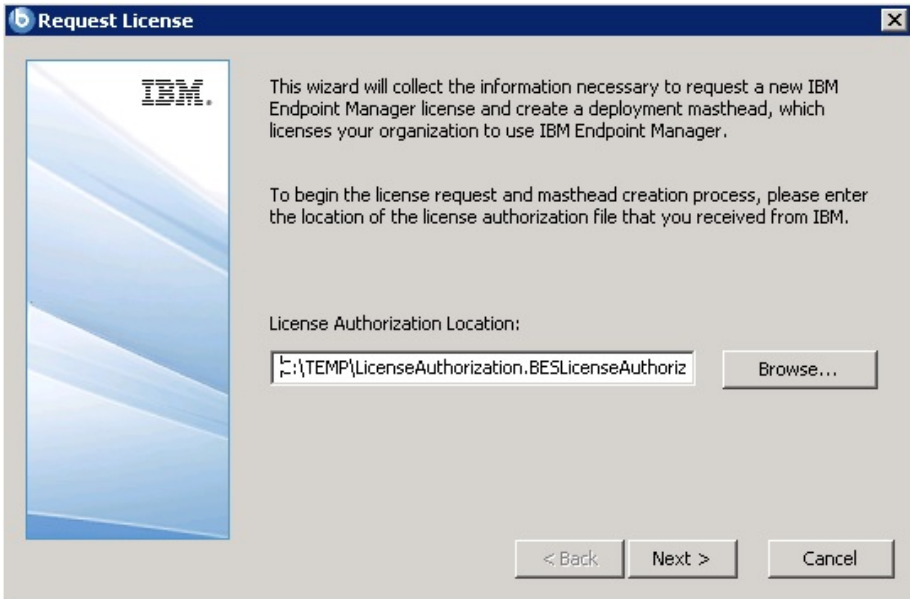

Figura 17. Solicitud de Licencia. (Vásquez Villacreses, 2015) (IBM, 2013)

4. Especifique un nombre **DNS** o la **dirección IP** de su servidor y haga clic en Siguiente.

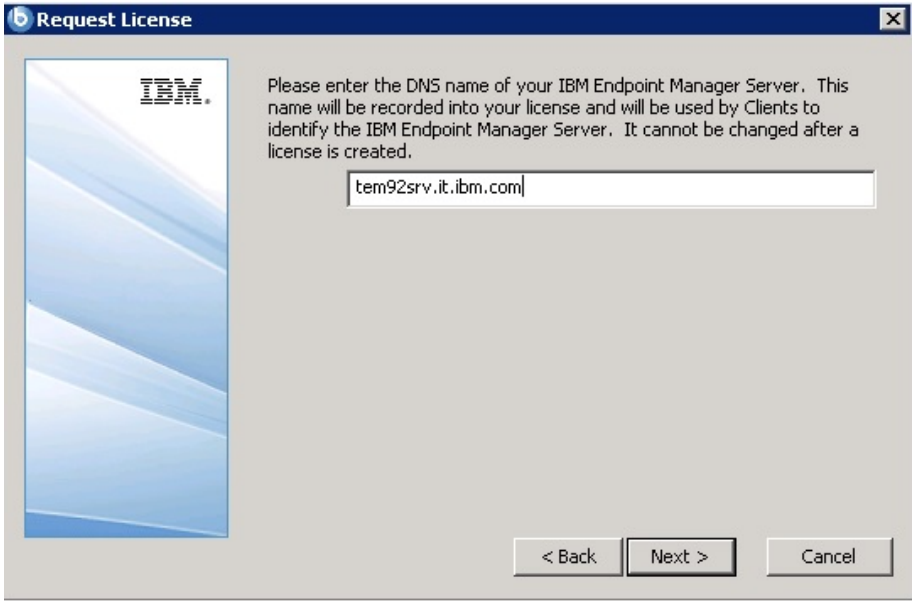

Figura 18. Credenciales del Servidor. (Vásquez Villacreses, 2015) (IBM, 2013)

Recomendación: Se debe ingresar un nombre DNS, como bes.companyname.com, debido a su flexibilidad a la hora de cambiar los equipos servidor y hacer configuraciones de red avanzadas. Este nombre se registra en el certificado de licencia y es utilizado por los clientes para identificar el servidor. Una vez creado el certificado de licencia, el nombre DNS no se puede cambiar. Para cambiar el nombre DNS, se debe solicitar un nuevo certificado de licencia, lo que requiere una nueva instalación.

5. Se escribe una contraseña de administrador del sitio para su despliegue. La contraseña se ingresa dos veces (para la verificación), y con un tamaño de clave (de 2K a 4K bits) para cifrar el archivo de clave privada. Damos clic en Crear.

Figura 19. Generación de claves pública / privada. (Vásquez Villacreses, 2015) (IBM, 2013)

De esta manera se genera un par de claves pública / privada utilizada para crear y autorizar todos los usuarios de Endpoint.

6. Guardamos el archivo de clave privada (license.pvk) en una carpeta con permisos de acceso o en una unidad extraíble, como un PGPDisk o una unidad USB. Hacemos clic en Aceptar.

   Recomendación: Si pierde el archivo de clave privada, un nuevo certificado de licencia tiene que ser creado, lo que requiere una nueva instalación. Además, cualquier persona con el archivo de la clave y la contraseña privada tiene un control total sobre todos los equipos con los clientes de IBM Endpoint Manager instalados por lo cual es recomendable mantener el archivo de la clave privada y clave en un lugar seguro.

7. A continuación se pide enviar el archivo de solicitud de IBM para la verificación de licencia. Si se dispone de conexión a Internet, se debe seleccionar la opción de presentar la solicitud en internet. En este caso, un archivo de solicitud se envía a IBM para la verificación de licencia. Esta

solicitud consta de su archivo original de autorización, el nombre DNS del servidor y clave pública, todo empaquetado en un solo archivo.

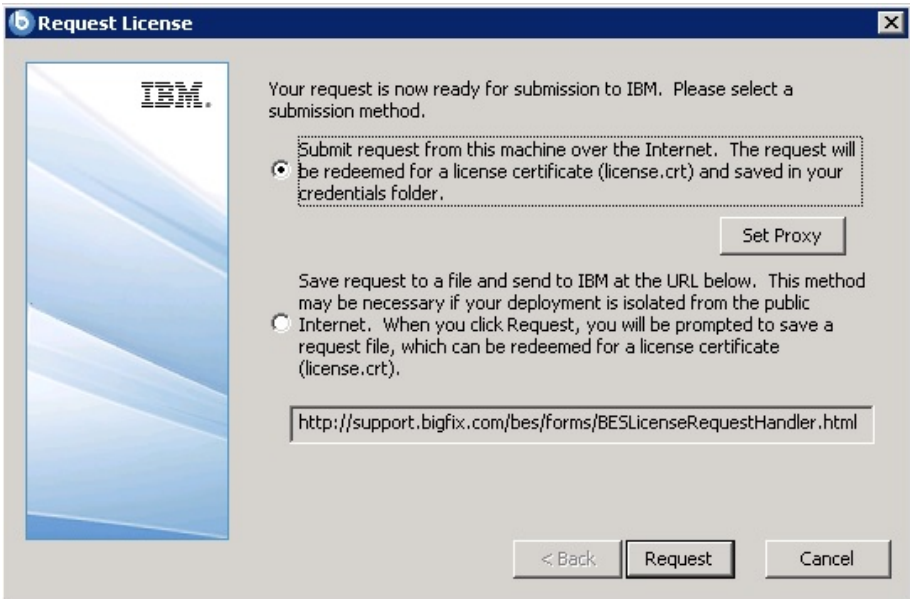

Figura 20. Verificación de archivo de la Licencia. (Vásquez Villacreses, 2015) (IBM, 2013)

8. Si se opta por presentar la solicitud a través de Internet y la empresa utiliza un servidor proxy para acceder a Internet, hacemos clic en Configurar Proxy para abrir el panel de configuración de proxy. En este panel se puede configurar la conexión proxy.

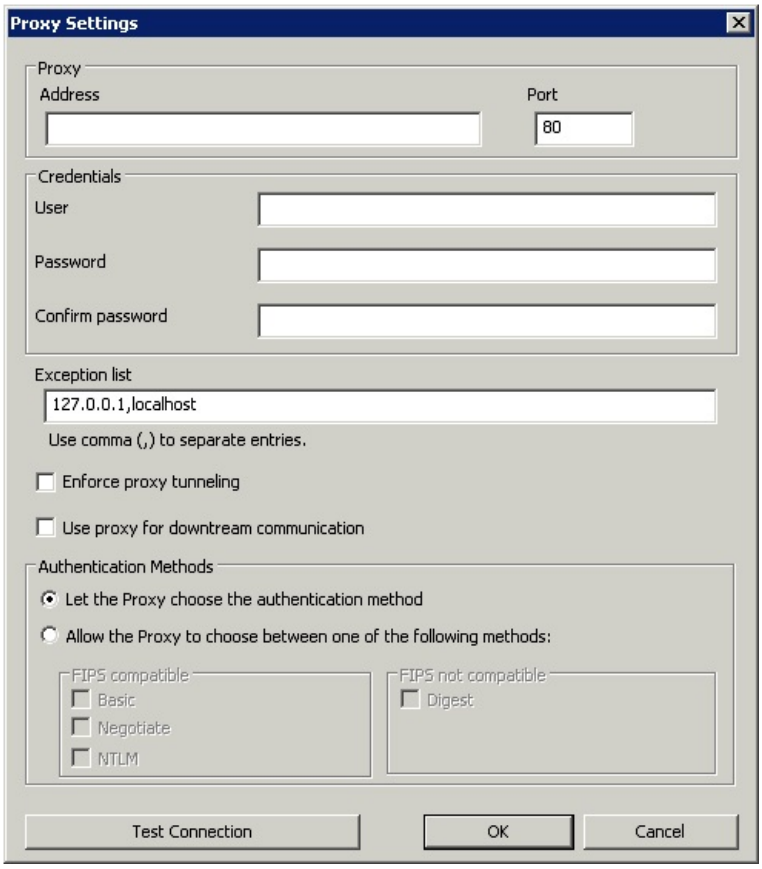

Figura 21. Especificaciones del Proxy. (Vásquez Villacreses, 2015) (IBM, 2013)

9. Se debe especificar:
    - El nombre de host o dirección IP y, opcionalmente, el puerto para comunicarse con la máquina proxy.
    - Las credenciales del usuario definido en la máquina proxy que deben utilizarse al establecer la conexión.
    - La lista separada por comas de nombres de host, subdominios, direcciones IP que identifican a los sistemas de la topología de IBM que no debe ser alcanzado a través del proxy. De forma predeterminada, IBM Endpoint Manager V9.2 evita desviar las comunicaciones internas hacia el proxy. Si se establece un valor en este campo, se sobrescribe el comportamiento por defecto. Para garantizar que las comunicaciones internas no están dirigidos al proxy, se debe agregar localhost, 127.0.0.1, yourdomain.com, Dirección_IP a la lista de excepciones que se especifican en este campo.

- Sea o no el proxy puede ser configurado para interconectarse mediante el uso de tunneling. Por defecto el proxy no realiza este tipo de interconexión.
- Se debe especificar el método de autenticación a utilizar al establecer la comunicación. Se puede dejar que el proxy escoja el método de autenticación o puede imponer el uso de métodos de autenticación específicos.

Recomendación: Si se desea habilitar el modo FIPS, se debe seleccionar un método de autenticación diferente a digest.

Se puede hacer clic en probar conexión para comprobar si la conexión con el proxy fue configurado con éxito.

Hacemos clic en Aceptar para guardar los ajustes y volver al panel de solicitud de licencia.

10. Hacemos clic en Solicitar. El Asistente recuperara su certificado de licencia (license.crt) desde el servidor de licencias de IBM Endpoint Manager.

    Alternativamente, si no se dispone de conexión a Internet, se debe seleccionar la opción de guardar la solicitud como un archivo llamado request.BESLicenseRequest. Copiamos el archivo en un equipo con conexión a Internet y enviamos la solicitud a la dirección URL de la página web de Endpoint que nos indica el instalador. La página ofrece un archivo license.crt. Copiamos el archivo de nuevo al equipo de instalación y lo importamos en el instalador.
11. Desde el diálogo de solicitud de licencia, hacemos clic en Crear para crear el archivo de cabecera.

Figura 22. Creación de archivo de Licencia. (Vásquez Villacreses, 2015) (IBM, 2013)

12. Se introducen los parámetros del archivo de cabecera que contiene información de configuración y la licencia junto con una clave pública que se utiliza para verificar la firma digital. Este archivo se guarda en la carpeta de credenciales.

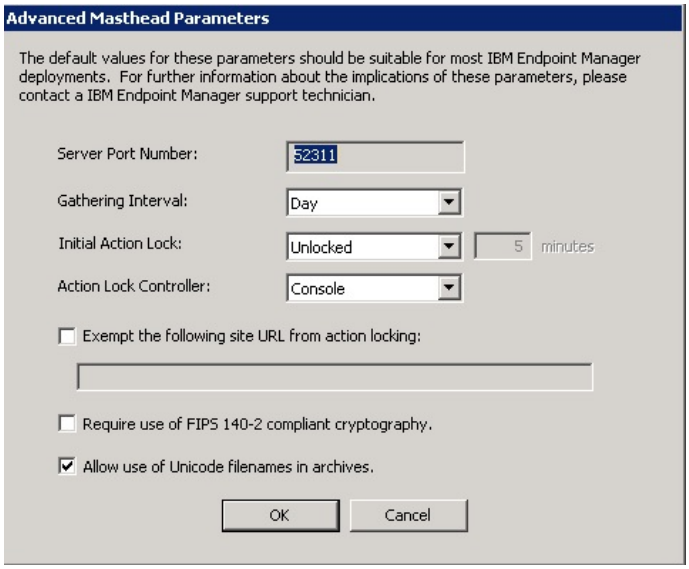

Figura 23. Configuración Avanzada de la Cabecera. (Vásquez Villacreses, 2015) (IBM, 2013)

En esta pantalla se pueden configurar las siguientes opciones:

Server Port Number: En general, no es necesario cambiarlo. Por defecto el puerto recomendado es el 52311, pero se puede elegir un puerto diferente si es más conveniente para la red particular. Normalmente, se elige un puerto

de la gama de puertos privados (49152 a 65535). También se puede utilizar un número de puerto reservado (puertos 1-1024), pero esto podría reducir la capacidad de controlar o restringir el tráfico correctamente y se impide el uso de números de puertos para aplicaciones específicas. Si se decide cambiar después de la implementación de los clientes, IBM Endpoint Manager no funcionará correctamente.

Recomendación: No se debe utilizar el número de puerto 52314 para la comunicación de red entre los componentes del Endpoint Manager, ya que está reservado para los agentes de proxy.

Gathering Interval: Esta opción determina el tiempo que los clientes esperan sin escuchar desde el servidor antes de que se compruebe si el nuevo contenido está disponible. En general, cada vez que el servidor recoge nuevos contenidos, intenta notificar a los clientes que el nuevo contenido se encuentra disponible a través de una conexión UDP. Sin embargo, en algunas situaciones las conexiones UDP están bloqueadas por los cortafuegos o cuando la traducción de direcciones de red (NAT) vuelve a asignar la dirección IP del cliente desde la perspectiva servidores, un intervalo más pequeño imperativo para obtener una respuesta oportuna de los clientes. Mayores tasas de recolección afectan ligeramente el rendimiento del servidor, ya que sólo se recolectan las diferencias; no se recolecta información de un cliente que ya se lo posee.

Initial Action Lock: Se puede especificar el estado de bloqueo inicial de todos los clientes, si se desea bloquear un cliente automáticamente después de la instalación. Los clientes bloqueados informan que los mensajes Fixlet son relevantes para ellos, pero no se aplican las acciones. El valor predeterminado es desbloqueado para bloquear los clientes de forma específica más adelante. Sin embargo, es posible que se desee comenzar con los clientes bloqueados y luego desbloquearlos de forma individual para dar más control sobre los clientes recién instalados. Como alternativa, se puede configurar los clientes para ser bloqueado por un cierto período de tiempo (en minutos).

Exempt the following site URL from action locking: En casos particulares, puede que se tenga que excluir a una URL específica de cualquier acción de

bloqueo para lo cual se debe marcar esta casilla e introducir la URL que se va a excluir.

Require use of FIPS 140-2 compliant cryptography: Marcamos esta casilla para cumplir con la normativa Federal Information Processing Standard (FIPS) en la red. Esto cambia la cabecera de modo que todos los componentes de IBM Endpoint se preconfiguran en modo FIPS. Por defecto, el cliente continúa en modo no FIPS si no se logra configurar correctamente FIPS, lo que podría ser un problema con los sistemas operativos heredados. Hay que tener en cuenta que marcar esta casilla puede agregar unos pocos segundos para el tiempo de arranque del cliente.

Allow use of Unicode filenames in archives: Esta configuración especifica la página de códigos utilizada para escribir los nombres de archivo en los archivos de IBM Endpoint. Se debe marcar esta casilla para escribir los nombres de archivo de página de códigos UTF-8.

Realizamos clic en Aceptar.

13. Finalmente se selecciona la carpeta en la que instalar los componentes de IBM Endpoint Manager.

3.3.3. Consola de administración

La consola de IBM Endpoint permite al personal de TI operar y solucionar problemas en todos los equipos administrados a través de la red. Se puede instalar en cualquier ordenador que puede hacer una conexión de red a través de HTTPS usando el puerto 52311 por defecto para el servidor. Salvo en los entornos de prueba o evaluación, no se recomienda ejecutar la consola en el equipo servidor debido a las implicaciones de rendimiento y seguridad al tener las credenciales clave en un equipo que ejecuta el servidor de base de datos o en la web.

Para instalar la consola, debemos realizar los siguientes pasos:

1. Ejecutar la Guía de instalación (Inicio> Programas> Administrador de IBM Endpoint> Guía de instalación de IBM Endpoint Manager). Hacemos clic en Instalar Componentes de IBM Endpoint Manager.
2. Desde el siguiente panel, damos clic en Instalar consola.

3. Cuando se le solicite, se debe introducir la ubicación de instalación de la consola. La ubicación predeterminada es `%PROGRAM FILES%\BigFix Enterprise\ConsolaBES`. Para elegir otro destino, se debe seleccionar Examinar y se va a la ubicación deseada. Hacemos clic en Siguiente para continuar.
4. Después de instalar los archivos, se debe seleccionar Finalizar para completar la instalación. Ahora se puede optar por iniciar la consola para instalar o gestionar los clientes.

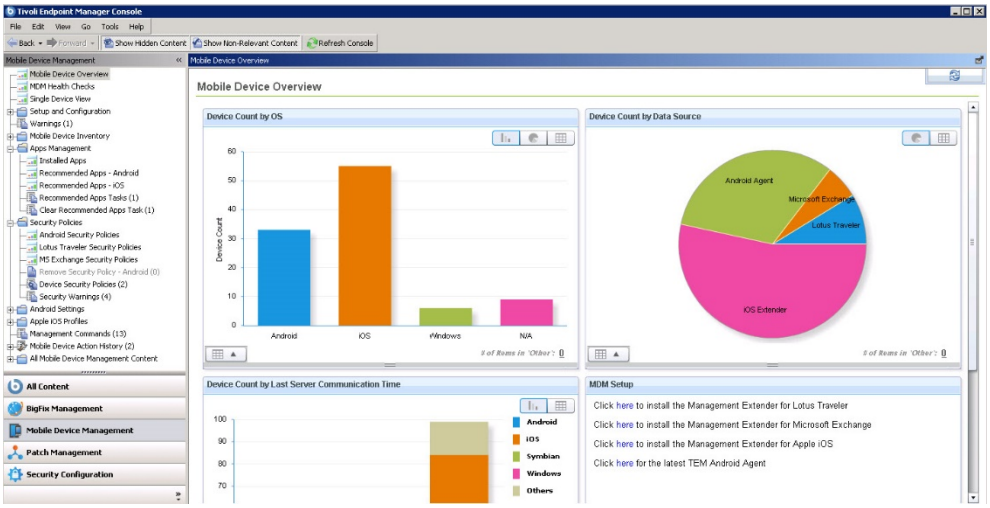

Figura 24. Consola de Administración de IBM Endpoint Manager. *(Vásquez Villacreses, 2015) (IBM, 2013)*

3.4.DESPLIEGUE DE AGENTES.

El despliegue de los clientes en todos los equipos de la red que se desea administrar, incluyendo el equipo que ejecuta la consola permite que el equipo reciba mensajes Fixlet importantes, como los parches de seguridad, archivos de configuración o actualizaciones.

Desde la consola, se debe seleccionar Install IBM Endpoint Manager Components> Install Clients> Install locally; para instalar el cliente en el equipo de manera local en el directorio que se desea especificar.

Adicionalmente se puede hacer uso de la herramienta de despliegue de cliente (BESClientDeploy.exe), con la cual se puede implementar los clientes de tres maneras:

Encontrar ordenadores mediante Active Directory: la herramienta de despliegue se comunica con el servidor de Active Directory para obtener una lista de todos los

equipos del dominio. Se comprueba cada uno de los ordenadores para ver si el cliente ya está instalado y muestra esta información en una lista.

Encontrar los ordenadores que utilizan Dominio NT 4.0: Todos los equipos del dominio se muestran con un indicador de estado que indica si está instalado el cliente.

Encontrar equipos especificados en una lista: está basado en la forma en que la red resuelve las direcciones de los equipos, se debe proporcionar una lista de nombres de equipos, rangos de direcciones IP o nombres de host. La lista debe tener rango de un nombre / dirección IP / nombre de host por línea. Con esta opción, la herramienta de despliegue no intenta descubrir todos los equipos, pero en su lugar intenta instalar directamente a todos los equipos enumerados.

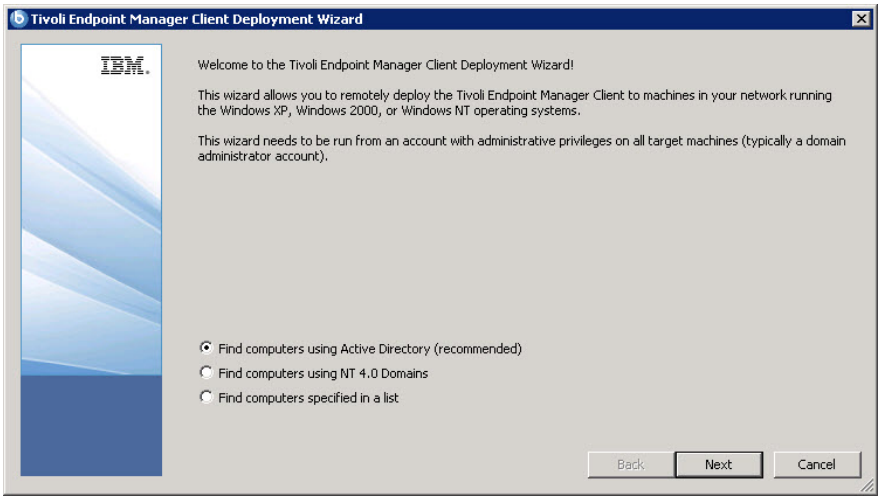

Figura 25. Asistente de Despliegue. *(Vásquez Villacreses, 2015) (IBM, 2013)*

3.4.1. Windows

Para el despliegue en Windows se puede usar la versión de Microsoft Installer (MSI) del cliente para interpretar el paquete y realizar la instalación de forma automática. Esta versión MSI del cliente (BESClientMSI.msi) se almacena en diferentes carpetas dependiendo si el servidor esta instalado en Windows o Linux:

Servidor Windows: `\BESInstallers\ClientMSI`

Servidor Linux: `/ServerInstaller.x86_64/repos/ClientMSI`

Para instalar el cliente en Windows debemos seguir los siguientes pasos:

1. Copiar el programa `BESClientMSI.msi` en la carpeta `c:\BESInstallers\ ClientMSI` si no existe es necesario crearla.
2. Ejecutar el programa `BESClientMSI.msi`
3. Finalmente debemos iniciar el servicio del cliente BES.

3.4.2. Android

Para realizar el despliegue del agente en Android debemos tener en cuenta la versión de en nuestro dispositivo ya que los requisitos mínimos para la instalación del agente es Android 2.2.; tras validar lo anterior seguimos los siguientes pasos:

1. Desde el dispositivo móvil, se ingresa a Google Play y se busca “IBM Mobile Client”.
2. Después de instalar debemos aceptar los permisos para la aplicación (la aplicación necesita varios permisos para gestionar el dispositivo móvil) y damos clic en “Activar” para permitir que el agente de Android tenga permisos de administrador.
3. Al iniciar la aplicación, se debe ingresar el nombre del servidor, dirección de correo del usuario; los datos son en relación si el dispositivo es de propiedad del usuario o de la organización ya que permite orientar las políticas de seguridad.

   La dirección del servidor introducido en el cuadro debe ser accesible en la red por el dispositivo y no es necesario especificar el número de puerto en el caso de utilizar los valores por defecto (52311). Si durante la instalación se especificó un número de puerto diferente se debe introducir el número de puerto (por ejemplo, mdm.companyname.com:12345).

   La dirección de correo electrónico se informa como el "nombre de usuario" en la consola de BigFix.

   Si el usuario selecciona que el dispositivo es "personal", a continuación, el seguimiento de localización se desactiva automáticamente. La propiedad del dispositivo es visible en la Consola de BigFix y se puede utilizar para orientar las políticas a los dispositivos.
4. Cuando el usuario hace clic en "Conectar", el Agente Android descargará el archivo de cabecera desde el servidor. Después se enrolarse con éxito la cabecera, funcionará muy similar a cualquier otro agente BigFix.

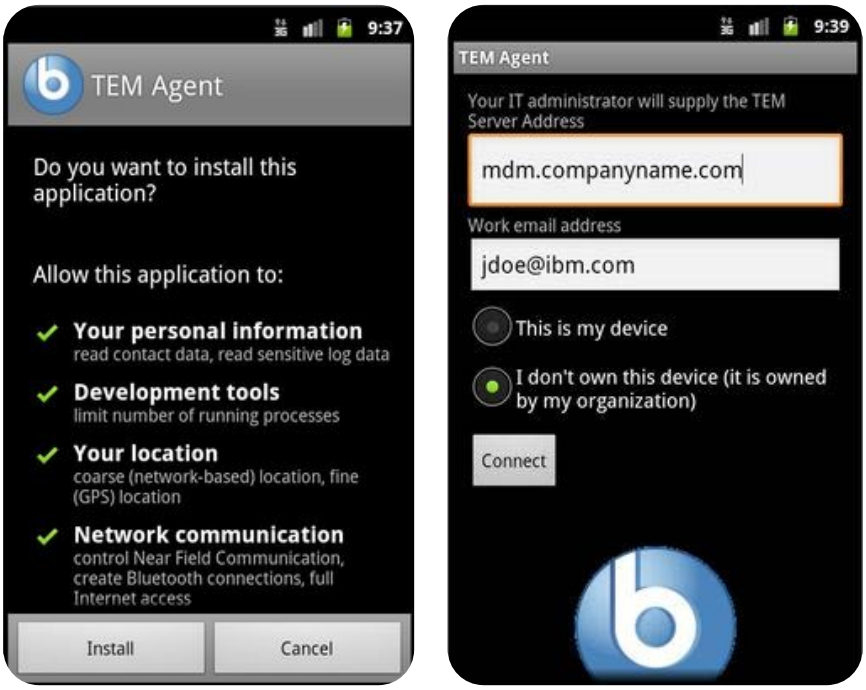

Figura 26. Despliegue Agente Android. *(IBM, 2015)*

3.5. TAREAS COMUNES.

Al finalizar la instalación es aconsejable comprobar que los servicios asociados a la herramienta están desplegados e iniciados correctamente, para lo cual debemos ejecutar desde la línea de comandos o consola lo siguiente:

Tabla 14.

Comandos para iniciar / detener los servicios de IBM Endpoint Manager

INICIAR SERVICIOS IBM ENDPOINT MANAGER

SERVIDOR WINDOWS	SERVIDOR LINUX
BES Root Service	service besserver start
BES FillDB	service besfilldb start
BES GatherDB	service besgatherdb start
BES Client	service beswebreports start
BES Web Reports Service	service besclient start

DETENER SERVICIOS DE IBM ENDPOINT MANAGER

SERVIDOR WINDOWS	SERVIDOR LINUX
BES Web Reports Service	service besclient stop
BES Client	service beswebreports stop
BES GatherDB	service besgatherdb stop
BES FillDB	service besfilldb stop
BES Root Service	service besserver stop

Recuperado de: *(IBM, 2015)*

3.5.1. Inventario de Hardware

Para realizar el inventario de dispositivos finales es necesario realizar el descubrimiento de dichos dispositivos para lo cual TEM ofrece varias formas de identificar los equipos que no tienen instalado el cliente:

Despliegue del Agente: el agente es la herramienta que se conectará con Active Directory ya sea por protocolo LDAP u OpenLDAP y comprobará si los equipos tienen el servicio Cliente TEM en ejecución. La herramienta de implementación del agente viene incluido al crear el generador de la instalación y se puede utilizar para instalar el cliente TEM si los equipos están en el dominio de Active Directory.

Descubrimiento de Activos usando Fixlet en Sitio: Un Fixlet en Sitio permite implementar de forma remota "Puntos de Scan" para escudriñar periódicamente las subredes remotas y luego importar los datos en la consola de TEM.

El uso del segundo método permite el descubrimiento e identificar dispositivos de red como routers, impresoras, y los interruptores que no pueden tener instalado el cliente TEM.

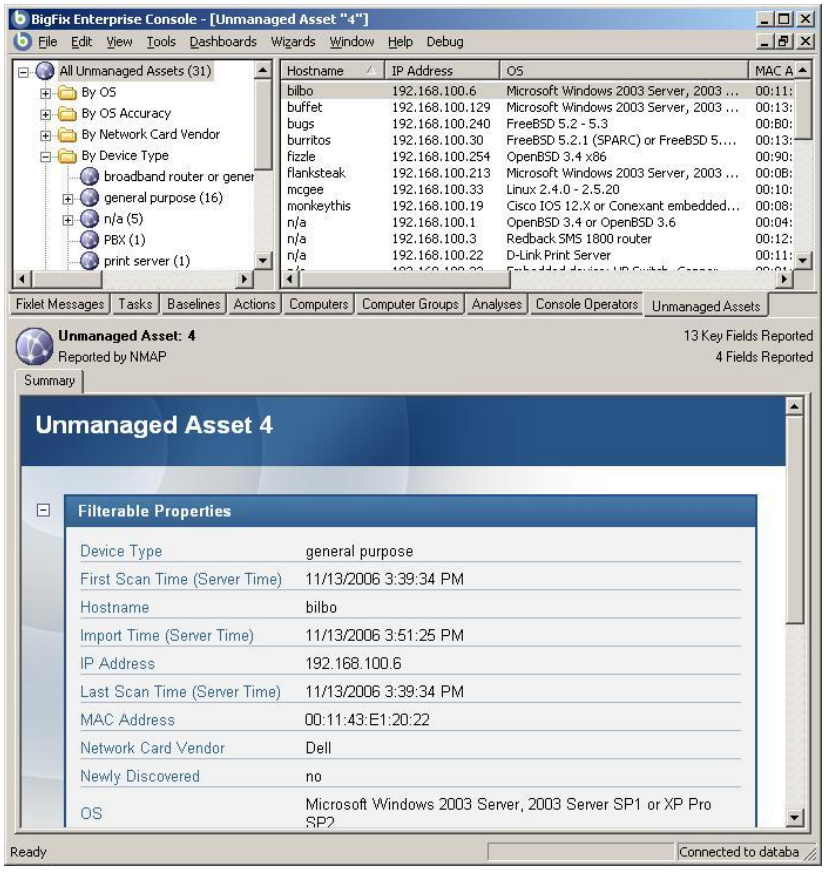

Figura 27. Consola de Administración de Hardware. *(IBM, 2015)*

3.5.2. Inventario de Software

El administrador de dispositivos puede identificar el software con y sin licencia de una organización con una amplia granularidad para rastrear los patrones de uso del software y las tendencias a través de equipos con Windows, UNIX y Linux. Reduciendo drásticamente el tiempo necesario para llevar a cabo un inventario exhaustivo de activos de software con fines de reconciliación licencia o de normativas de cumplimiento, la solución proporciona información valiosa sobre lo que la organización posee y lo que se ha instalado, junto con qué frecuencia el software está siendo utilizado con el fin de apoyar una mejor planificación, elaboración de presupuestos y licenciamiento con el proveedor de cumplimiento y auditoria.

El inventario del software que cada equipo contiene se lo puede encontrar en la ventana de administración de activos. (IBM, 2015)

3.6. ACCIONES DE GESTIÓN.

IBM Endpoint Manager para dispositivos móviles permite a los administradores o usuarios finales a través de un portal de autoservicio personalizado borrar de forma remota datos de teléfonos y tabletas. Las opciones disponibles en dispositivos específicos variarán según la plataforma, versión del sistema operativo, y el método de gestión.

3.6.1. Borrado Remoto

El comando "Borrar" se utiliza para restablecer un dispositivo a "ajustes de fábrica" por el borrado de todos los datos de la memoria interna del dispositivo (el almacenamiento externo en la tarjeta SD no se suele eliminar). Este comando se utiliza normalmente cuando un dispositivo se pierde o es robado y necesita todos los datos para ser eliminados.

Después de limpiar un dispositivo, el dispositivo vuelve a su estado de fábrica y ya no puede ser administrado por IBM Endpoint Manager; a menos que se lo reconfigure para la gestión.

3.6.2. Bloqueo

Cuando un dispositivo esta enrolado a la plataforma se puede enviar mensajes a dispositivos móviles que tengan el cliente IBM Mobile. Para poder enviar mensajes:

Android utiliza "notificaciones" para mensajería del usuario final. La notificación se quedará en la barra de estado del sistema Android hasta que el usuario abra y revise la notificación. Los mensajes para Android son controlados en la pestaña "Mensajes" de la ventana de dialogo "Take Action".

El envío de mensajes personalizados permite conectar cualquier acción como puede ser el bloqueo del equipo; o también se puede enviar con una "acción en blanco" para mostrar sólo el mensaje.

Otra forma de enviar mensajes es a través de Fixlet mediante el cual algunos mensajes Fixlet tendrán acciones que enviarán mensajes al cliente móvil de forma predeterminada. Se puede utilizar los mensajes predeterminados o modificarlos usando la pestaña “Mensajes” de la ventana de dialogo “Take Action”.

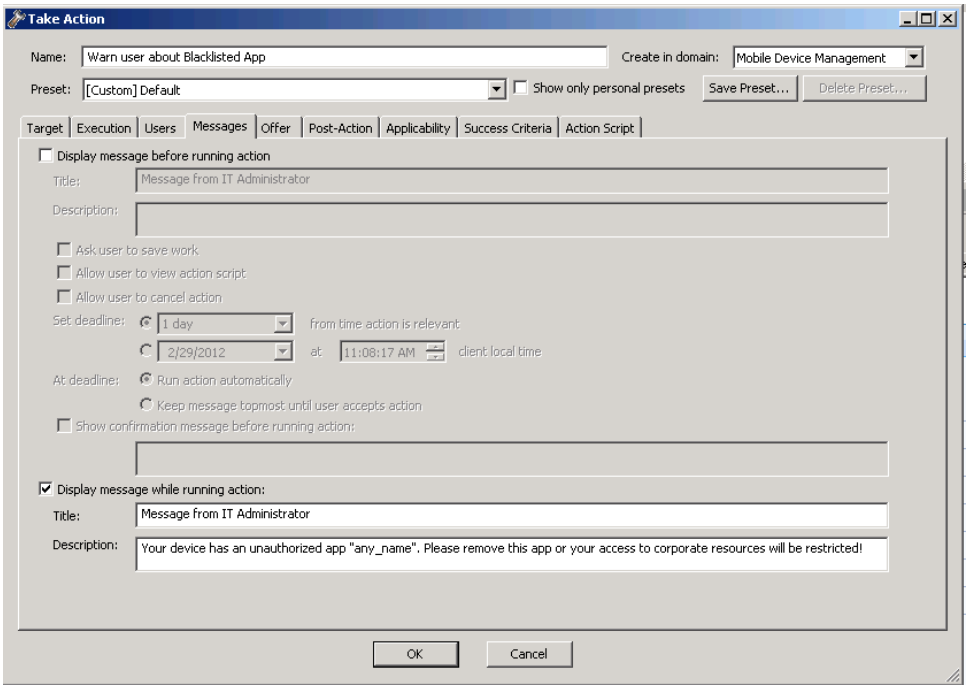

Figura 28. Envío de Mensajes a Dispositivos Móviles. *(Vásquez Villacreses, 2015) (IBM, 2013)*

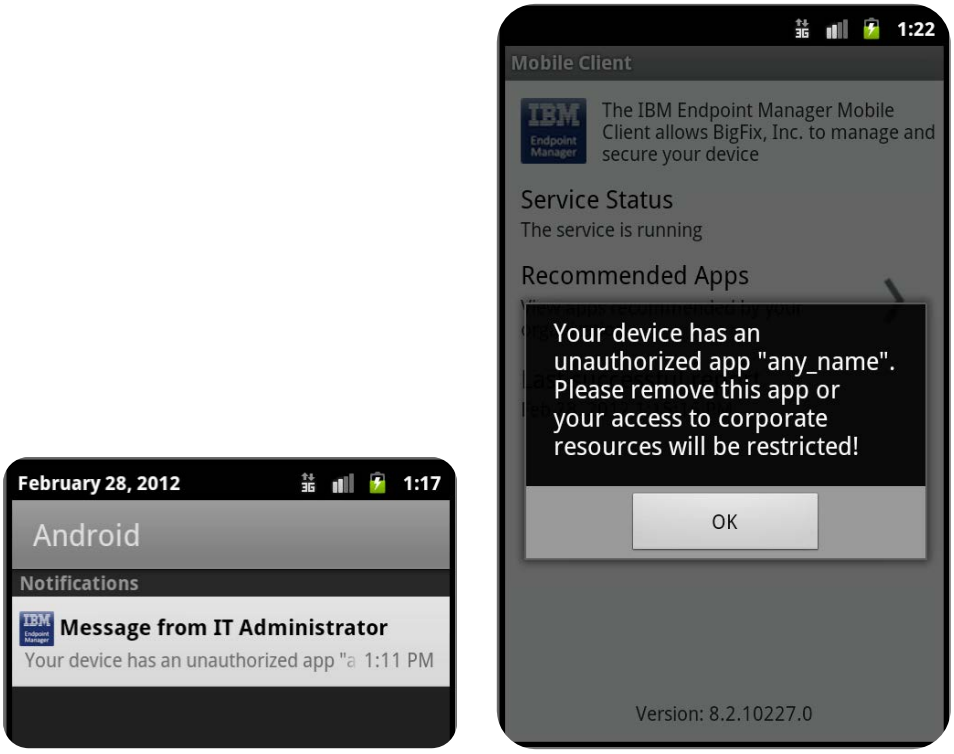

Figura 29. Mensajes y acciones en dispositivos Android. *(IBM, 2015)*

3.7. CONFIGURACIÓN DE SEGURIDAD.

Para alcanzar y mantener el cumplimiento requiere de recursos para optimizar el tiempo y esfuerzo invertido por las operaciones, auditoría de TI y los equipos de seguridad. A menudo, las operaciones y los equipos de seguridad están enfocados a un ambiente reaccionario, escalonado a la seguridad, en lugar de un enfoque sin fisuras con una visión y presentación de informes unificado.

3.8. ADMINISTRADOR DE POLÍTICAS DE SEGURIDAD.

Para la gestión de las políticas de seguridad existen dos dominios desde la consola de administración de la seguridad:

- Configuración de la seguridad.
- Endpoint Protection.

El dominio de configuración de la seguridad proporciona acceso a los contenidos de configuración de seguridad tales como descubrimiento de activo, gestión de la configuración y vulnerabilidades.

3.9. PERMISOS DE USUARIOS.

Para instalar y mantener Tivoli Endpoint Manager suele requerir la cooperación de varios administradores y operadores para lo cual se utilizara la herramienta de administración y gestión de usuarios la misma que facilitara la creación de los usuarios administradores y gestión de roles. Para cada usuario se debe ingresar el nombre, correo, contraseña y permisos.

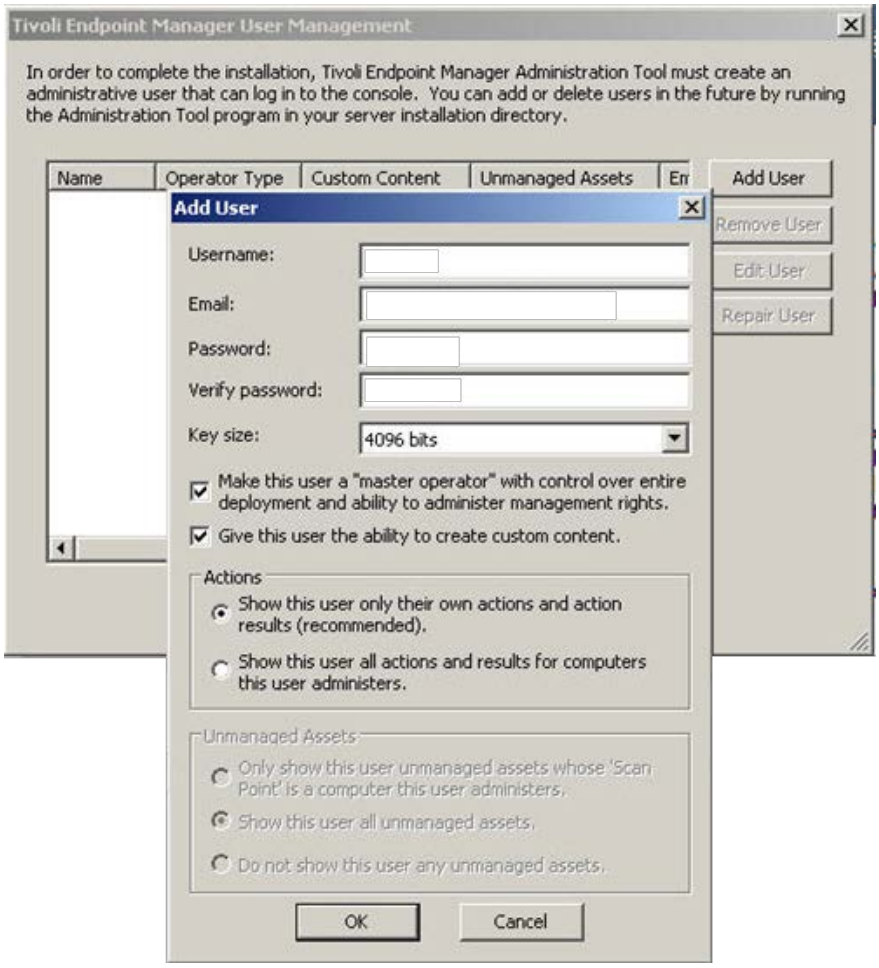

Figura 30. Herramienta de Administración de usuarios. *(IBM, 2015)*

Al iniciar un despliegue de Tivoli Endpoint Manager, se solicita la integración con servidores de dominio para facilitar la gestión de usuarios con lo cual cada usuario heredará los permisos y roles configurados en el directorio activo.

CAPÍTULO 4. RENTABILIDAD.

4.1. INTRODUCCIÓN.

Se puede definir a la rentabilidad como el beneficio que una empresa obtiene al realizar una inversión de un recurso financiero; el mismo que se puede obtener de tres maneras:

- *Por parte del capital de la empresa:* es todo aquel recurso que se obtiene por parte de los accionistas.
- *Adquisición de una deuda:* es el mecanismo por el cual se obtiene recursos financieros o tangibles haciendo uso de los acreedores.
- *Uso de las reservas:* que son recursos que ha retenido la empresa como resultado de ejercicios anteriores con el fin de autofinanciarse, cabe tener en cuenta que el uso de las reservas debe estar apoyado en un estudio a fondo de la inversión para evitar la inestabilidad de la misma.

Aclarando este concepto y después de haber analizado en los anteriores capítulos las características de las plataformas de seguridad de la información y al postura que se debe adoptar para la correcta adopción de las políticas de BYOD, trataremos en este capítulo la rentabilidad en las empresas al acoger políticas adecuadas y la aplicación de buenas prácticas para hacer de BYOD una herramientas de productividad.

4.2. RENTABILIDAD A LAS EMPRESAS.

Los "requisitos de negocio" de la compañía debe estar direccionada en evaluar y analizar los desafíos de mejora de la productividad tomando decisiones que permitan incrementar su competitividad; para lo cual se debe tener visibilidad de los proyectos y procesos que facilitan la optimización de recursos en el área de tecnología de la información.

La generación de rentabilidad de la implementación de una nueva tecnología debe cumplir varios requisitos como son:

- Conocer adecuadamente los procesos relacionados de la empresa.
- Planificar detalladamente los requerimientos y necesidades.

Al planificar se debe contemplar un crecimiento paulatino de los sistemas de información ya que lo que se pretende es una convergencia del costo total de propiedad de

los activos de los sistemas con la postura de seguridad de la empresa; la misma que se ve reflejada en el grado de madurez de la misma.

De acuerdo con Carlo Angeles de la Oficina Nacional de Gobierno Electronico e informática del Péru: "El desarrollo de una infraestructura de Información debe tener consideraciones estratégicas, un planeamiento detallado con participación de todas las áreas de la organización. Si la empresa desea explotar las TI como una oportunidad estratégica de beneficio de la organización, la alta dirección debe realizar un proceso de planeamiento estratégico con el fin de determinar hacia dónde se orientará el negocio y cuál será su nuevo reposicionamiento a fin de que los planes estratégicos de la función que administra las TI sean coherentes y de un adecuado soporte a las estrategias empresariales". (Angeles, 2010)

4.2.1. Retorno de la inversión - ROI

ROI también conocido como el retorno de la inversión es el término inglés con el cual es comúnmente conocida la rentabilidad económica.

De acuerdo con la oficina OCW[35] de la Universidad Carlos III de Madrid: "A veces se utilizan los términos ingleses para referirnos a la rentabilidad económica: Return on Assets (ROA) o Return on Investments (ROI)", en el cual utilizamos el beneficio económico como medida de beneficios y el activo total o pasivo total como medida de recursos utilizados.

$$RE = \frac{BE\ (Beneficio\ Económico)}{AT\ (Activo\ Total)}$$

Ecuación 1. Rentabilidad Económica. *(OpenCurseWare, 2015)*

En donde el beneficio económico son todos los ingresos percibidos por la empresa sustrayendo los costos exceptuando los intereses de deudas e impuestos.

Teniendo en cuenta que el beneficio neto se lo obtiene al sustraer del beneficio económico el interés por deudas e impuestos, se puede obtener también la rentabilidad financiera:

[35] (OpenCurseWare, 2015). **OCW:** Es la base de conocimiento conocida como OpenCurseWare de diferentes áreas de docencia de la Universidad Carlos III de Madrid, ofreciendo acceso libre y gratuito a los materiales de una muestra de cursos.

$$RF = \frac{BN\ (Beneficio\ Neto)}{K\ (Fondos\ Propios: Capital + Reserva)}$$

Ecuación 2. Rentabilidad Financiera. *(OpenCurseWare, 2015)*

De acuerdo con estudios realizados por la empresa de investigación Forrester en su estudio realizado para BIM que lleva el título de: "The Total Economic Impact Of IBM Managed Mobility for BYOD", nos indica que la implementación de políticas de servicios móviles permite aumentar la rentabilidad de la empresa por la agregación de varios beneficios:

- *Productividad de los empleados (69,3% de beneficios):* el trabajo efectivo se incrementa ya que se puede acceder a la información donde sea y en cualquier momento.
- *Aumento de los ingresos por la mejora en la movilidad de las ventas (6,8% de beneficio):* la introducción de BYOD al departamento de ventas de una organización aumentan la cantidad de clientes atendidos, y permite la generación de negocios a tiempo real.
- *Reducción de costos en servicios móviles (17,3% de beneficios):* la reducción en la adquisición de dispositivos móviles corporativos permite un ahorro operativo en la implementación de servicios e instalación ($350 en promedio por dispositivo) y reduce los consumos de datos y voz corporativos ($90 por dispositivo).
- *Disminución del almacenaje de equipos y costos de reposición (0,9% de beneficios):* al disminuir la adquisición de dispositivos por parte de la empresa se evita gastos de almacenaje que pueden llegar a los $25 por equipo.
- *Reducción de la infraestructura y soporte a dispositivos móviles (5,6% de beneficio):* al amenorar la cantidad de dispositivos empresariales, los costos de soporte y mantenimiento de los equipos se ve reducida.
- *Mejora la productividad de Help Desk (0,2% de beneficios):* al manejar la empresa dispositivos de propiedad de los usuarios, se encuentran bajo el soporte de las empresas proveedoras de servicios móviles (datos y voz), reduciendo el trabajo operativo por parte del soporte interno de las empresas.

Como resultado de la implementación de una política de BYOD la empresa debe incurrir en gastos de implementación y operativos:

- *Implementación interna (0,9% de costos):* representa los costos iniciales que el departamento de IT incurre al realizar pruebas de infraestructura y despliegue.
- *Licenciamiento y cargos por servicios (19,5% de costos):* la empresa debe adquirir herramientas para gestionar los servicios móviles y licenciamiento mensual.
- *Servicios Inalámbrico (79,1% de costos):* para los dispositivos enrolados en las políticas de BYOD las empresas pagan una cuota mensual a las operadoras para garantizar la continuidad del plan de datos en dichos dispositivos ($85 al mes por dispositivo).
- *Planificación y gestión (0,6% de costos):* son los costos que llevan la implementación de una plataforma cruzada que permita al departamento de IT el despliegue de la herramienta a lo largo de varias plataformas de los dispositivos.

En adición se puede observar el análisis financiero realizado con respecto a los datos obtenidos en el estudio realizado por **Forrester Consulting**[36], el cual fue solicitado por IBM para analizar el retorno de la inversión frente a la aplicación de políticas BYOD:

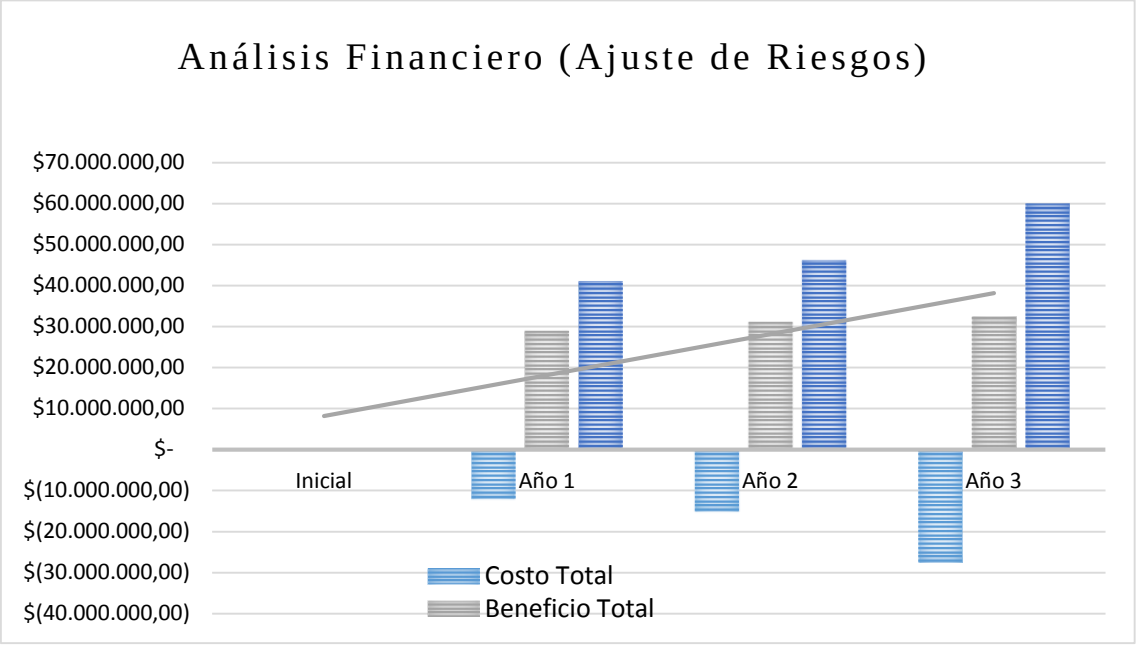

Figura 31. Resumen Financiero 3 años- (riesgo Ajustado). *(Forrester)*

[36] **ACLARACIÓN:** Todas las figuras y las tablas mostradas han sido tomados del caso de estudio de Forrester los mismos que son redondeados y obtenidos de empresas de Estado Unidos y cuya moneda es el USD Dólar Norte americano.

Tabla 15.

Supuestos del modelo

Ref.	Métrica	Cálculo	Valor
A1	Horas de trabajo al año.		2080
A2	Salario Ejecutivo Completo.		$ 280.000
A3	Costo por hora Ejecutivo.	A2/A1	$ 135
A4	Salario Empleado completo.		$ 120.000
A5	Costo por hora Empleado.	A4/A1	$ 58
A6	Salario Help Desk completo		$ 80.000
A7	Costo por hora Help Desk.	A6/A1	$ 38

Recuperado de: *(Forrester)*

Tabla 16.

Costos de implementación interna - Sin riesgo - ajustados

Ref	**Métrica**	**Cálculo**	**Inicial**	**Año 1**	**Año 2**	**Año 3**
B1	Duración de la implementación inicial (semanas).		12			
B2	Número de empleados involucrados en la implementación inicial.		15			
B3	Horas usadas por empleado a la semana.		25			
B4	Costo hora del empleado.	A5	$ 58			
B5	Licenciamiento y costo de Hardware VDI.			$ 20.000		
B6	Duración de la implementación VDI (semanas).			4		
B7	Número de empleados involucrados en la implementación VDI.			4		
B8	Horas usadas por empleado a la semana en implementación VDI.			20		
B9	Costo por hora Empleado.	A5		$ 58		
BT	Costos Totales.	(B1*B2*B3*B4)+B5+ (B6*B7*B8*B9)	$ (261.000)	$ (38.560)		

Recuperado de: *(Forrester)*

Tabla 17.

Licenciamiento BYOD y costos de servicios - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Inicial	Año 1	Año 2	Año 3
C1	Número de dispositivos registrados para BYOD.		100	9000	11000	12500
C2	Licenciamiento mensual y costo de servicio por dispositivo registrado.		$ 21	$ 21	$ 21	$ 21
C3	Número de meses.		6	12	12	12
CT	Costos Totales.	C1*C2*C3	$ (12.600)	$ (2.268.000)	$ (2.772.000)	$ (3.150.000)

Recuperado de: *(Forrester)*

Tabla 18.

Costo de servicio inalámbrico - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Inicial	Año 1	Año 2	Año 3
D1	Número de dispositivos registrados para BYOD.		100	9000	11000	12500
D2	Licenciamiento mensual y costo de servicio por dispositivo registrado.		$ 90	$ 85	$ 85	$ 85
D3	Número de meses.		6	12	12	12
DT	Costos Totales.	D1*D2*D3	$ (54.000)	$ (9.180.000)	$ (11.220.000)	$ (12.750.000)

Recuperado de: *(Forrester)*

Tabla 19.

Costos de gestión y planificación programadas - sin riesgo - ajustados

Ref	Métrica	Cálculo	Inicial	Año 1	Año 2	Año 3
E1	Número de empleados involucrados.		7	7	7	7
E2	Horas usadas por empleado a la semana.		5	3	3	3
E3	Número de semanas.		24	48	48	48
E4	Costo por hora Empleado.	A5	$ 58	$ 58	$ 58	$ 58
ET	Costos Totales	E1*E2*E3*E4	$ (48.720)	$ (58.464)	$ (58.464)	$ (58.464)

Recuperado de: *(Forrester)*

Tabla 20.

Costos totales - Sin riesgo - ajustados

Costos	Inicial	Año 1	Año 2	Año 3	Total	Valor Actual
Implementación interna.	($ 261.000)	($ 38.560)	$ 0	$ 0	($ 299.560)	($ 296.055)
Licenciamiento BYOD y Servicios	($ 12.600)	($ 2.268.000)	($ 2.772.000)	($ 3.150.000)	($ 8.202.600)	($ 6.731.969)
Costos Servicios inalámbricos.	($ 54.000)	($ 9.180.000)	($ 11.220.000)	($ 12.750.000)	($ 33.204.000)	($ 27.251.446)
Costos de gestión y planificación.	($ 48.720)	($ 58.464)	($ 58.464)	($ 58.464)	($ 224.112)	($ 194.111)
Costos Totales.	($ 376.320)	($ 11.545.024)	($ 14.050.464)	($ 15.958.464)	($ 41.930.272)	($ 34.473.580)

Recuperado de: *(Forrester)*

Tabla 21.

Incremento de productividad empleados - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Inicial	Año 1	Año 2	Año 3
F1	Dispositivos registrados en BYOD.		100	9.000	11.000	12.500
F2	Porcentaje de dispositivos usados en actividades de trabajo.		98%	95%	92%	90%
F3	Minutos adicionales trabajados por semana por empleado registrado en BYOD.		60	55	50	45
F4	Número de semanas.		24	48	48	48
F5	Costos por hora Empleado.	Inicial: A3 Años 1-3: A5	$ 135	$ 58	$ 58	$ 58
FT	Total	F1*F2*(F3/60) *F4*F5	$ 317. 520	$ 21.819.600	$ 23.478.400	$ 23.490.000

Recuperado de: *(Forrester)*

Tabla 22.

Ingresos ampliados por mejora en movilidad de ventas - Sin riesgo -ajustados

Ref	Métrica	Cálculo	Año 1	Año 2	Año 3
G1	Número de tabletas registradas en BYOD.		900	1.100	1.250
G2	Porcentaje de tabletas usadas en ventas.		25%	22%	20%
G3	Oportunidad de ingresos incrementales por uso de tabletas en ventas.		$ 7.500	$ 9.500	$ 11.500
GT	Total	G1*G2*G3	$ 1.687.500	$ 2.299.000	$ 2.875.000

Recuperado de: *(Forrester)*

Tabla 23.

Reducción de dispositivos móviles y servicios corporativos - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Año 1	Año 2	Año 3
H1	Número de dispositivos nuevos emitidos antes de BYOD.		250	250	250
H2	Costo de adquisición e instalación por dispositivo.		$ 350	$ 350	$ 350
H3	Número de dispositivos sin BYOD		5.000	5.250	5.500
H4	Cargos mensuales de voz y datos por dispositivo.		$ 90	$ 90	$ 90
H5	Meses al año		12	12	12
HT	Total	(H1*H2)+(H3*H4*H5)	$ 5.487.500	$ 5.757.500	$ 6.027.500

Recuperado de: *(Forrester)*

Tabla 24.

Disminución de inventario de dispositivos y costo de reposición - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Año 1	Año 2	Año 3
I1	Número de dispositivos sin BYOD.		5.000	5.250	5.500
I2	Porcentaje de dispositivos que necesitan un cambio o actualización.		15%	15%	15%
I3	Costo promedio por dispositivo cambiado o actualizado.		$ 250	$ 250	$ 250
I4	Número de dispositivos con BYOD.		1.200	800	500
I5	Número de dispositivos corporativos eliminados de BYOD.	I1-I4	3.800	4.450	5.000
I6	Gastos generales de almacenaje por dispositivo.		$ 25	$ 25	$ 25
IT	Total	(I1*I2*I3)+(I5*I6)	$ 282.500	$ 308.125	$ 331.250

Recuperado de: *(Forrester)*

Tabla 25.

Reducción de infraestructura móvil y costos de soporte - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Año 1	Año 2	Año 3
J1	Costo anual de servidores e infraestructura sin BYOD.		$ 15.000	$ 16.500	$ 18.150
J2	Costo anual de servidores e infraestructura con BYOD.		$ 6.000	$ 6.000	$ 6.000
J3	Número de empleados de IT para infraestructura sin BYOD.		5	5	5
J4	Número de empleados de IT para infraestructura con BYOD.		2	2	2
J5	Porcentaje de tiempo empleado en mantenimiento.		75%	75%	75%
J6	Salario completo de empleados.		$ 120.000	$ 120.000	$ 120.000
J7	Número de dispositivos sin BYOD.		5.000	5.250	5.500
J8	Licenciamiento mensual por dispositivo corporativo.		$ 25	$ 25	$ 25
J9	Meses al año.		12	12	12
JT	Total	(J1-J2)+((J3-J4)*J5*J6)+(J7*J8*J9)	$ 1.779.000	$ 1.855.500	$ 1.932.150

Recuperado de: *(Forrester)*

Tabla 26.

Mejora en la productividad de HelpDesk - Sin riesgo - ajustados

Ref	Métrica	Cálculo	Año 1	Año 2	Año 3
K1	Número de dispositivos corporativos sin BYOD.		5.000	5.250	5.500
K2	Número de dispositivos corporativos con BYOD.		1.200	800	500
K3	Número de dispositivos corporativos eliminados de BYOD.	K1-K2	3.800	4.450	5.000
K4	Volumen de llamadas a HelpDesk por dispositivo.		2	2	2
K5	Duración promedio de cada llamada (minutos).		12	12	12
K6	Costo por hora HelpDesk.	A7	$ 38	$ 38	$ 38
IT	Total	K3*K4*(K5/60)*K6	$ 57.760	$ 67.640	$ 76.000

Recuperado de: *(Forrester)*

Tabla 27.

Beneficios totales - Sin riesgo - ajustados

Beneficio	Inicial	Año 1	Año 2	Año 3	Total	Valor Actual
Incremento de productividad.	$ 317.520	$ 21.819.600	$ 23.478.400	$ 23.490.000	$ 69.105.520	$ 57.205.541
Ingresos ampliados en ventas.	$ 0	$ 1.687.500	$ 2.299.000	$ 2.875.000	$ 6.861.500	$ 5.594.121
Reducción de dispositivos móviles y costos de servicio.	$ 0	$ 5.487.500	$ 5.757.500	$ 6.027.500	$ 17.272.500	$ 14.275.451
Reducción de inventario y costos por reemplazo.	$ 0	$ 282.500	$ 308.125	$ 331.250	$ 921.875	$ 760.340
Reducción de infraestructura móvil y costos de soporte.	$ 0	$ 1.779.000	$ 1.855.500	$ 1.932.150	$ 5.566.650	$ 4.602.397
Mejora en productividad HelpDesk	$ 0	$ 57.760	$ 67.6440	$ 76.000	$ 201.400	$ 165.510
Total beneficios.	$ 317.520	$ 31.113.860	$ 33.766.165	$ 34.731.900	$ 99.929.445	$ 82.603.359
Número de usuarios / dispositivos BYOD	100	9.000	11.000	12.500	32.600	N/A
Promedio beneficios / usuarios	$ 3.175	$ 3.457	$ 3.070	$ 2.779	$ 3.065	$ 2.534

Recuperado de: *(Forrester)*

Tabla 28.

Ajustes por riesgo de costos y beneficios

Costo	Bajo	Lo más probable	Alto	Significado
Implementación internacional.	100%	100%	125%	108%
Licencias BYOD y servicios.	100%	100%	125%	108%
Servicios Inalámbricos.	100%	100%	125%	108%
Planificación de programas y Gestión.	100%	100%	125%	108%

Beneficio	Bajo	Lo más probable	Alto	Significado
Incremento de productividad.	80%	100%	103%	94%
Ingresos ampliados por movilidad en ventas.	50%	100%	110%	87%
Reducción de dispositivos y costos de servicios.	80%	100%	103%	94%
Reducción de inventario y costos por reemplazo.	92%	100%	105%	99%
Reducción de infraestructura móvil y costos de soporte.	80%	100%	103%	94%
Mejora en productividad HelpDesk.	80%	100%	103%	94%

Recuperado de: *(Forrester)*

Tabla 29.

Flujo de fondos - Sin riesgo - ajustados

	Inicial	Año 1	Año 2	Año 3	Total	Valor Actual
Costos.	($ 376.320)	($ 11.545.024)	($ 14.050.464)	($ 15.958.464)	($ 41.930.272)	($ 34.473.580)
Beneficios.	$ 317.520	$ 31.113.860	$ 33.766.165	$ 34.731.900	$ 99.929.445	$ 82.603.359
No Beneficios.	($ 58.800)	$ 19.568.836	$ 19.715.701	$ 18.773.436	$ 57.999.173	$ 48.129.779
ROI.	140%					
Periodo de Recuperación.	< 1 mes					

Recuperado de: *(Forrester)*

Tabla 30.

Resumen por usuario - Sin riesgo - ajustados

	Inicial	Año 1	Año 2	Año 3	Total Promedio
Costo por usuario	($ 3.763)	($ 1.283)	($ 1.277)	($ 1.277)	($ 1.286)
Beneficio por usuario.	$ 3.175	$ 3.457	$ 3.070	$ 2.779	$ 3.065
Sin beneficio por usuario.	($ 588)	$ 2.174	$ 1.792	$ 1.502	$ 1.779

Recuperado de: *(Forrester)*

4.3. LICENCIAMIENTO.

Para un ambiente inicial de implementación de la solución de IBM Endpoint Manager es necesario el licenciamiento de los siguientes componentes:

- Clientes (Nodos).
- Servidores.
- Retransmisores.
- Consola de Administración.

Acorde con el esquema de la infraestructura de la empresa, y alineado con las necesidades iniciales se adquiere IEM Core Protection el mismo que nos permite realizar un descubrimiento de la red, análisis de comportamiento a nivel local, despliegue de firewall a nivel de dispositivo y final y proporciona una seguridad en la navegación mediante el análisis de reputación web y descarga de archivos.

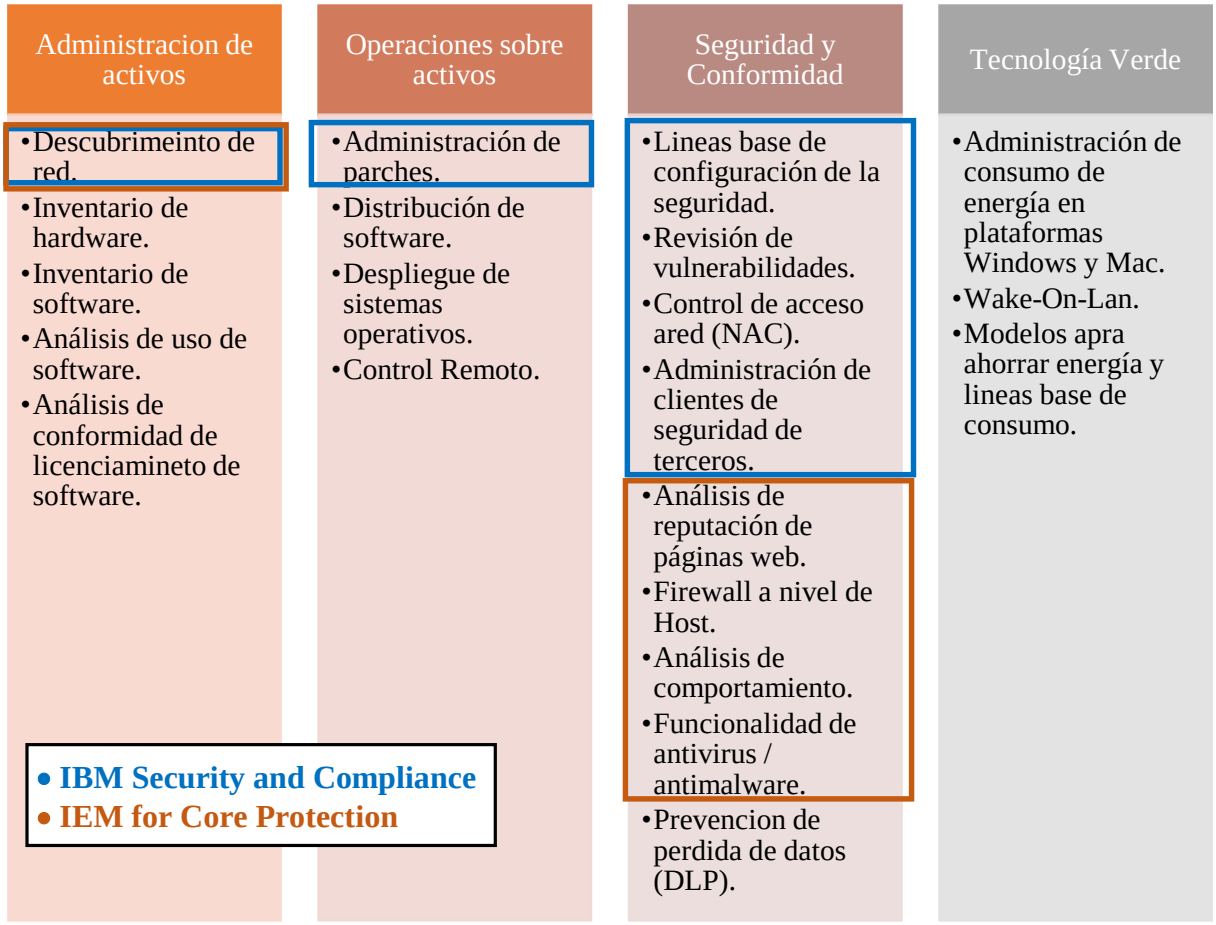

Tabla 31. Licenciamiento y funcionalidades de IBM TEM. *(Darnalt C. , 2013)*

4.4. CAPACITACIÓN AL PERSONAL DE IT.

El factor decisivo que se encuentra por debajo de una implementación en el área de TI, es el recurso humano, por tal motivo es imprescindible mantener el soporte a usuario.

Es conveniente establecer los requerimientos de los usuarios de la manera más precisa posible y definir los alcances que se pueden llegar con la gestión del soporte para mitigar falsas expectativas por parte del usuario.

4.4.1. Mejores Prácticas

Durante el levantamiento de requerimientos a usuarios se puede servir de plantillas, normativas o prácticas de gestión de infraestructura como es ITIL; en cuya metodología se puede establecer niveles de soporte por cada grupo de usuario.

En el momento de implementación de las políticas de BYOD es necesario definir los grupos de trabajo, teniendo en cuenta que es un proceso de gestión del cambio que impactara de forma positiva o negativa a la empresa según como se le plantee.

Después de tener claro que grupo de trabajo iniciará el proyecto es importante establecer una estrategia para la seguridad basada en los riesgos que se definen en la fase de planificación. La seguridad es uno de los mayores factores decisivos por los cuales una empresa puede aprobar o no la adopción de BYOD.

Es recomendable establecer de forma inteligente los requerimientos de los sistemas para la adopción de una plataforma que nos permita la gestión centralizada y la integración con soluciones actuales; creando en base a los riesgos los controles de seguridad que se deben implementar.

CONCLUSIONES Y RECOMENDACIONES.

CONCLUSIONES.

1. La implementación de seguridad en los dispositivos móviles no debe ser un obstáculo para la aceptación de BYOD, ya que se puede crear un ambiente hibrido en el cual coexistan políticas de seguridad a nivel empresarial con las necesidades de los usuarios; impulsando la productividad del empleado dejando a un lado la espontaneidad para tener una planificación estratégica.
2. La tendencia de BYOD nos permite aprovechar los avances tecnológicos que se están dando en nuestros tiempos como son la introducción y evolución de los smartphones y la aparición de nuevos gadget tecnológicos que nos permiten mejorar nuestra productividad.
3. Los beneficios que obtienen las empresas al permitir el ingreso de dispositivos inteligentes por parte de los empleados se traduce en un ahorro significativo al prescindir de dispositivos cuya vida útil es corta debido a la constante actualización de los mismos.
4. Una de las ventajas que se puede obtener es el incremento de la satisfacción por parte de los trabajadores al poder utilizar dispositivos con los cuales son familiares y que operan en el día a día, sin tomar en cuenta los ahorros que se incurren al evadir los gastos operativos de capacitaciones e inducciones de utilización de estos dispositivos, permitiendo así tener usuarios más contentos y satisfechos en su trabajo.
5. IBM es una empresa de hardware y software en la cual se tuvo experiencia laboral, lo cual me sirvió para familiarizarme con los temas tratados en la presente disertación.
6. Las redes corporativas contienen información muy valiosa para las empresas y la implementación de herramientas de seguridad no debe ser tomada a la ligera por parte del departamento de IT ya que se debe asegurar la confidencialidad, disponibilidad e integridad de la información que se maneja.
7. La solución propuesta por IBM para la gestión y administración de dispositivos finales es adaptable al giro de negocio de la empresa permitiendo agregar módulos acorde a las futuras necesidades. Sin embargo la versión que se tomó para el caso de estudio (v8.02), carece de la integración con soluciones de seguridad de terceros.

8. La seguridad en puntos finales es el comienzo de una estrategia de postura de seguridad frente al costo de propiedad que toda empresa debe valorar, ya que inicialmente los sistemas se encontraran segregados por silos, cada fabricante tendrá una solución por segmento a proteger y lo óptimo es la interoperabilidad y gestión centralizada de todos estos sistemas.
9. La herramienta seleccionada permite el control granular y la integración con más módulos y soluciones del mismo fabricante; permitiendo cubrir gran parte del espectro de la empresa, a diferencia que las soluciones de otros fabricantes son puntuales para secciones del giro de negocio.

RECOMENDACIONES.

1. Al tratarse de una tendencia que está en constante crecimiento se debe poner en consideración que los sistemas de seguridad se encuentran desarrollados para mitigar las amenazas y salvaguardar la información importante y se debe complementar con una cultura de seguridad y mejores prácticas a los empleados para atenuar las brechas de seguridad.
2. El presupuesto de la mayor parte de las empresas ecuatorianas no permite la implantación de soluciones cuyo nicho de mercado son empresas multinacionales; como es el caso de IBM Endpoint Manager, para lo cual es recomendable recurrir a soluciones cuya implementación inicial sean más económicas y permitan un crecimiento modular y granularidad que va acorde al nivel de madurez de las empresas ecuatorianas.
3. Se recomienda asignar gran parte del tiempo de elaboración del proyecto en la preparación de buenas prácticas y documentar los procesos de forma ordenada y entendible; los mismos que sean de conocimiento público dentro de la empresa y puedan ser accedidos por todos los usuarios mediante portales internos fomentando la colaboración entre usuarios.
4. Hoy en día los dispositivos móviles están en apogeo y la tecnología está en constante crecimiento haciendo que la movilidad en el trabajo sea lo cotidiano haciendo de esto una ventaja competitiva, por tal motivo la adopción no BYOD no es algo mandatorio; es un modelo de movilidad que complementa el giro del negocio y que debe ser evaluado ya que existen varios modelos que pueden encajar de mejor forma en cada empresa, como lo son la implementación de ambientes híbridos.

5. Es necesario delimitar de la mejor forma los dispositivos finales, sistemas operativos y conjunto de aplicaciones que van a encontrarse inmersos en las políticas de BYOD para evitar costos innecesarios que podrían provenir del incremento de dispositivos dando lugar a la insatisfacción de los usuarios por estar fuera de soporte.
6. Es recomendable realizar el análisis de las demás herramientas por un periodo de al menos 30 días para poder comprender de mejor manera las utilidades que nos brindan así como al configuración adecuada de sus políticas de seguridad.

BIBLIOGRAFÍA.

Angeles, C. (Diciembre de 2010). *Gestión de procesos y productividad con tecnologías de la información.* Obtenido de http://www.ongei.gob.pe/estudios/publica/estudios/t02_opt_negtic_dic2010.pdf

Apple. (4 de Marzo de 2015). *Volume Program for Business*. Obtenido de http://www.apple.com/business/vpp/

Arntz, P. (11 de Mayo de 2013). *What is Host Intrusion Prevention*. Obtenido de https://blog.malwarebytes.org/intelligence/2013/05/whatiships/

CATEDU. (12 de Febrero de 2015). *Plataforma E-Ducativa*. Obtenido de http://e-ducativa.catedu.es/44700165/aula/archivos/repositorio//1000/1057/html/22_componentes_tcnicos_arquitectura_clienteservidor.html

CCN-CERT 401. (2014). *Glosario y Abreviaturas.* España: Centro Criptológico Nacional.

CCN-CERT IA-21/13. (2013). *Riesgos y amenazas del BYOD.* España: Centro Criptológico Nacional.

CCN-STIC-450. (2013). *Guía de Seguridad de las TIC.* España: Centro Criptológico Nacional.

Cisco. (2008). *Guía de estudio de CCNA Exploration: Conceptos y protocolos de enrutamiento.* Estados Unidos: Prentice-Hall.

Cisco. (2012). *BYOD - Cisco IBSG Horizons.* Obtenido de http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons-Global_ES.pdf

Citrix. (2014). *XenMobile*. Obtenido de http://lac.citrix.com/products/xenmobile/overview.html

Cross Check Networks. (2005- 2013). *SOA Testing Techniques.* Obtenido de http://www.crosschecknet.com/soa_testing_black_white_gray_box.php

Darnalt, C. (2013). IBM Security Solutions (ISS). Bogotá, Colombia.

Darnalt, C. (2013). Un vistazo a la computacíon en la nube. Manuscrito no publicado. Bogotá, Colombia.

DeBeasi, K. D. (Octubre de 2011). Managing Employee-Owned Technology in the Enterprise. (G. Group, Entrevistador)

DELL. (22 de 01 de 2013). *Global BYOD Survey Result.* Obtenido de http://www

ESET Latinoamérica. (2012). *Eset LA.* Obtenido de http://www.welivesecurity.com/wp-content/uploads/2014/01/documento_guia_byod_W.pdf

Forrester, C. (s.f.). The Total Economic Impact Of IBM Managed Mobility for BYOD. Cambridge, Massachusetts, Estados Unidos.

Fundación Wikimedia, Inc. (Enero de 2015). *Localizador de recursos uniforme*. Obtenido de http://es.wikipedia.org/wiki/Localizador_de_recursos_uniforme

Garcia, S. (18 de Enero de 2009). *Aplicaciones Distribuidas.* Obtenido de http://es.slideshare.net/soreygarcia/aplicaciones-distribuidas-presentation

Gartner, Inc. (2014). *Gartner Security & Risk Management Summit*. Obtenido de http://www.gartner.com/technology/summits/na/security/

Gartner, Inc. (2015). *Gartner Consulting*. Obtenido de http://www.gartner.com/technology/home.jsp

Goncalves, M. (1997). *Firewalls Complete.* E.E.U.U.: McGraw Hill.

Haletky, E. (Enero de 2013). *Trend Micro Deep Security Reference.* Obtenido de https://enterprise.apac.trendmicro.com/deepsecurity/content/3-Deep_Security_additional_info/WP_DeepSecurity_Reference_Architecture_HybirdCloud_130116_US_Final.pdf

IBM. (Septiembre de 2013). IBM Endpoint Manager 8.2 PoC. Quito, Pichincha, Ecuador.

IBM. (2014). *IBM Tivoli Software*. Obtenido de https://www.ibm.com/software/tivoli

IBM. (10 de Septiembre de 2015). *IBM Big Fix Inventory.* Obtenido de http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_TI_SE_USEN&htmlfid=TID14086USEN&attachment=TID14086USEN.PDF

IBM. (08 de Septiembre de 2015). *IBM Developer Works*. Obtenido de https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Endpoint%20Manager/page/Asset%20Discovery

IBM. (Febrero de 2015). *IBM Endpoint Manager family*. Obtenido de http://www-03.ibm.com/software/products/es/endpoint-manager-family

IBM. (05 de Abril de 2015). *IBM Knowledge Center*. Obtenido de http://www-01.ibm.com/support/knowledgecenter/tivoli_iea/com.ibm.iea.tem/tem/8.2/configuration/client_auto_relay_select_relay_affiliation.pdf

IBM. (27 de Mayo de 2015). *IBM Support*. Obtenido de https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli+Endpoint+Manager/page/Fixlets

IBM. (12 de Septiembre de 2015). *Support BigFix.* Obtenido de http://support.bigfix.com/product/documents/Tivoli_Endpoint_Manager_Administrators_Guide_81.pdf

IBM Global Financing. (2015). *Lease or Purchase*. Obtenido de http://www-03.ibm.com/financing/us/leasevpur.html

IBM Knowledge Center. (27 de Mayo de 2015). *IBM*. Obtenido de http://www-01.ibm.com/support/docview.wss?uid=swg21684809

Informatica Hoy. (2012). *Informatica Hoy*. Obtenido de http://www.informatica-hoy.com.ar/aprender-informatica/Que-es--la-tecnologia-3G.php

ISO 27000.es. (2005). *ISO 27000 en Español*. Obtenido de http://www.iso27000.es/sgsi.html

ISO/IEC. (s.f.). *Information security management*. Obtenido de ISO/IEC 27001: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Kioskea. (Junio de 2014). *Kioskea: Entorno cliente/servidor*. Obtenido de http://es.kioskea.net/contents/148-entorno-cliente-servidor

Kioskea. (Febrero de 2015). *Kioskea.Net: LAN (Red de área local)*. Obtenido de http://es.kioskea.net/contents/253-lan-red-de-area-local

MaaS360. (2015). *MaaS360 Leads in the Mobile Cloud*. Obtenido de http://www.maas360.com/why-maas360/maas360-leads-in-the-mobile-cloud/?s=home

Microsoft. (2 de Septiembre de 2009). *Microsoft TechNet*. Obtenido de MDM Perimeter Network Configuration: https://technet.microsoft.com/en-us/library/dd261867.aspx

Moreno, M. G. (23 de Julio de 2013). *El BYOD (Bring Your Own Device) en la empresa. Retos legales y beneficios.* Écija: Editorial Aranzadi. Obtenido de http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/el-byod-bring-your-own-device-en-la-empresa-retos-legales-y-beneficios

Novell. (2015). *ZENworks Endpoint Security Management Overview*. Obtenido de https://www.novell.com/documentation/zesm35/install/data/bbimcpj.html

OpenCurseWare. (29 de 09 de 2015). *Universidad Carlos III de Madrid.* Obtenido de http://ocw.uc3m.es/economia-financiera-y-contabilidad/economia-de-la-empresa/material-de-clase-1/Rentabilidad.pdf

Optenet. (2015). *Internet Security Solutions for SaaS Service Providers*. Obtenido de http://www.optenet.com/en-us/solutions-saas-providers.asp

Osorio, J. (28 de Agosto de 2001). *Informática Cliente-Servidor*. Obtenido de http://www.angelfire.com/my/jimena/so2/com_guia2.htm

Oviedo, G. A. (19 de Marzo de 2013). *Software libre Vs. Software licenciado*. Obtenido de http://cdtiuniajc.blogspot.com/2013/03/programa-coti-21-marzo-2013.html

Preciado, F. H. (Febrero de 2015). *Concepto de Aplicaciones Distribuidas*. Obtenido de http://wikipiratasdeltec.wikispaces.com/Concepto+de+Aplicaciones+Distribuidas

Salesforce.com EMEA Limited. (2000 - 2015). *Introduction to CRM.* Obtenido de http://www.salesforce.com/uk/crm/what-is-crm.jsp

Software Guru. (Abril de 2013). *SG Buzz*. Obtenido de http://sg.com.mx/buzz/10-consejos-para-una-estrategia-byod

Story, A. (2009). *An alternative primer on national and international copyright law in the global South: eighteen questions and answers.* Canterbury, Kent: Universidad de Kent.

Symantec. (28 de Marzo de 2014). *How To Install and Configure Mobile Device Management* . Obtenido de http://www.symantec.com/connect/articles/how-install-and-configure-mobile-device-management-part-1-2

Symantec. (2 de Febrero de 2015). *Symantec Data Loss Prevention*. Obtenido de http://www.symantec.com/es/mx/data-loss-prevention/

Symantec. (2015). *Symantec Mobility: Suite*. Obtenido de http://www.symantec.com/es/mx/mobility/products/

The Open Group. (2011). *The Open Group*. Obtenido de http://www.opengroup.org/soa/source-book/soa/soa.htm

Trend Micro. (Enero de 2012). *Trend Micro Consumerization.* Obtenido de The cause and effect of consumerization in the worplace: http://uk.trendmicro.com/imperia/md/content/uk/about/consumerization/consumerization_exec_summary-en.pdf

Trend Micro. (Febrero de 2015). *Seguridad móvil y gestión de aplicaciones para BYOD*. Obtenido de http://www.trendmicro.es/productos/mobile-security/

TrendLabs. (2013). *Guía Electrónica para la Vida Digital*. Obtenido de TrendMicro: http://www.trendmicro.es/media/br/4ws-and-1h-of-mobile-privacy-es.pdf

Universidad d'Alacant. (2005). Programación en Internet. Alicante, San Vicente del Raspeig, España.

Vásquez, L. (2015). Disertación. Quito, Pichincha, Ecuador: Pontificia Universidad Católica del Ecuador.

Vmware Airwatch. (Febrero de 2015). *Bring Your Own Device (BYOD)*. Obtenido de AirWatch Mobile Device Management: http://www.air-watch.com/solutions/bring-your-own-device-byod

Wave, D. (1994). *QR Code*. Obtenido de http://www.qrcode.com/en/about/

WikiLibros. (Enero de 2014). *Seguridad Informática.* Obtenido de http://es.wikibooks.org/wiki/Seguridad_inform%C3%A1tica

Wikipedia. (Junio de 2009). *Wikipedia: Advanced Encryption Standard*. Obtenido de http://es.wikipedia.org/wiki/Advanced_Encryption_Standard

Wikipedia. (3 de Agosto de 2009). *Wikipedia: Calidad de Servicio*. Obtenido de http://es.wikipedia.org/wiki/Calidad_de_servicio

Wikipedia. (7 de Mayo de 2013). *Wikipedia: Federal Information Processing Standard*. Obtenido de http://es.wikipedia.org/wiki/Federal_Information_Processing_Standard

Wikipedia. (28 de Diciembre de 2013). *Wikipedia: SANS*. Obtenido de http://es.wikipedia.org/wiki/SANS_Institute

Wikipedia. (Junio de 2014). *Wikipedia: ERP*. Obtenido de http://es.wikipedia.org/wiki/Sistema_de_planificaci%C3%B3n_de_recursos_empresariales

Wikipedia. (20 de Diciembre de 2014). *Wikipedia: Middleware*. Obtenido de http://es.wikipedia.org/wiki/Middleware

Wikipedia. (21 de Octubre de 2014). *Wikipedia: Proveedor de servicios de Internet*. Obtenido de http://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet

Wikipedia. (Julio de 2014). *Wikipedia: Wi-Fi*. Obtenido de http://es.wikipedia.org/wiki/Wi-Fi

Wikipedia. (8 de Abril de 2015). *Wikipedia: API*. Obtenido de http://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones

Wikipedia. (10 de Febrero de 2015). *Wikipedia: Over-the-air programming*. Obtenido de http://en.wikipedia.org/wiki/Over-the-air_programming

Wikipedia. (1 de Marzo de 2015). *Wikipedia: SDK*. Obtenido de http://es.wikipedia.org/wiki/Kit_de_desarrollo_de_software

Wikipedia. (14 de Enero de 2015). *Wikipedia: Servicio General de Paquetes vía Radio*. Obtenido de http://es.wikipedia.org/wiki/Servicio_general_de_paquetes_v%C3%ADa_radio

Wikipedia. (29 de 09 de 2015). *Wikipedia: VDI*. Obtenido de https://en.wikipedia.org/wiki/Desktop_virtualization

Zambrano, R. (Agosto de 2012). *Delitos informáticos contemplados en la ley ecuatoriana.* Obtenido de http://www.cec.espol.edu.ec/blog/rzambrano/files/2012/08/DELITOS-INFORM%C3%81TICOS-CONTEMPLADOS-EN-LA-LEY-ECUATORIANA.pdf

Zuñiga, E. (15 de Noviembre de 2012). *AltoNivel*. Obtenido de http://www.altonivel.com.mx/24878-claves-para-comprender-y-aplicar-una-estrategia-byod.html